# TRANSPORTATION SECURITY: ARE OUR AIRPORTS SAFE?

## HEARING

BEFORE THE

## COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

MAY 13, 2015

## Serial No. 114–27

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

95–252 PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DeSAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

SEAN MCLAUGHLIN, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
JAMES ROBERTSON, *Staff Director for Transportation and Public Assets Subcommittee*
MICHAEL KIKO, *Professional Staff Member*
MELISSA BEAUMONT, *Clerk*

# CONTENTS

# TRANSPORTATION SECURITY: ARE OUR AIRPORTS SAFE?

**Wednesday, May 13, 2015**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, DC.

The Committee met, pursuant to notice, at 10:25 a.m., in room 2154, Rayburn House Office Building, Hon. Jason Chaffetz (chairman of the Committee) presiding.

Present: Representatives Chaffetz, Mica, Duncan, Jordan, Walberg, Amash, DesJarlais, Massie, Meadows, DeSantis, Buck, Walker, Blum, Hice, Grothman, Palmer, Cummings, Maloney, Norton, Clay, Lynch, Connolly, Duckworth, Kelly, Lawrence, DeSaulnier, and Lujan Grisham.

Chairman CHAFFETZ. The Committee on Oversight and Government Reform will come to order. Without objection the chair is authorized to declare a recess at any time.

We have an important hearing today dealing with the TSA. Airport security is pivotal to our Nation's safety and security. We appreciate the thousands and thousands of men and women who serve at the TSA. I think they work hard. They are dedicated. They are committed. They don't know what they are going to see. We have an inordinate amount of guns that are still trying to be taken through airports, weapons of all kinds. It's a very difficult situation with literally tens and tens of thousands of security badges that are out there.

We need to continue to have a good, vibrant discussion in this country about the safety and security of our airports and how to do that. And one of the things I like to say, and I've said it many times, and I'm sure I'll continue to say it is, we're different in this Nation in that we are self-critical. We do take a good, hard look at our security parameters and challenge the notion that the standard status quo is acceptable.

One of the things that stuck out to me in the 9/11 report, the commission that came together, is that often government lacks imagination, where terrorists and would-be nefarious characters who want to do harm and provide mayhem, death, and destruction to the United States of America will often be more creative than our security personnel. And so to have this type of discussion, it's good that we hear a variety of perspectives. We have had some good work from the inspector general. We have had good work from the GAO. We have a good perspective from others who have had to deal with highly targeted areas such as Israel. And that's the type of discussion we have today.

But it does require that we have a very good communication between the Congress and Homeland Security, specifically the TSA. We have had an exceptionally difficult time, exceptionally difficult time, getting information from the TSA on some very basic matters.

One of the things, for instance, that we asked for, this is a blank, ladies and gentlemen, this is a blank form, a blank form, not filled out, a blank form that people are to use as they assess security. We asked to see a copy of it. We were allowed to see it in camera, but members here were not allowed to see that. And so we asked for a copy of it. This is what they give us, 100 percent redacted. This is a blank form that they will not even allow Congress to see. Now, if that's the type of cooperation we're going to get from the TSA, we're going to have some very difficult times.

Now, we had invited Mr. Caraway, who is the acting administrator, to come before the Committee. At first we heard a variety of excuses. We needed more than 2 weeks. Then we had a big dustup because for weeks we had planned to do this, in fact, more than a month we had planned to do this. Felt that he as the acting administrator would be pivotal to this discussion.

But Homeland Security objected to Mr. Ron's presence on the panel. They felt that it was demeaning, demeaning, to actually have the acting administrator sit on the same panel as a nongovernment witness. That's absurd. That's offensive. It's a waste of the Committee's time. It's a waste of Congress' time. We don't need two panels to have this discussion. We want to have one panel.

Now, we had decided in a very bipartisan, mutual way, that cabinet level secretaries, if they come to testify before the Committee, will be the sole person to testify. If you're below a cabinet level secretary, we're not going to separate you out into your own panel. But the TSA, different than others that we have had—I would remind you that we have had a variety of other people come before this Committee who sit side-by-side with regular people from the outside, from the private sector—and so unfortunately the TSA has refused, and Mr. Carraway has refused the Committee's invitation to appear before Congress.

We have been working on this since the first part of April. They've had plenty of notice, and up until late, late, late yesterday, he was going to be here if it was a separate panel. But now because we are not going to waste this Committee's time, we are not going to waste members' time, they are not sitting here today, and we will have less of a hearing because of it. It's an embarrassment that they would do that. They made these decisions themselves, but that is not the way it's going to work around here.

TSA had said, well, maybe we'll give you somebody else. It's not the TSA's decision as to who Congress calls to testify. That is not their decision. It is the decision of Congress to understand and to be informed by those that they invite before Congress. But that's where we find ourselves today.

So with that I'm going to now yield to—I took a little extra time there with that explanation—but now I would like to now recognize the chairman of the Subcommittee on Transportation, Mr. Mica of Florida.

Mr. MICA. Thank you. Thank you, Mr. Chairman, and the Ranking Member for holding this meeting. I think it's an insult to the Committee that TSA would not send the acting administrator to this panel with due notice. This is a very important oversight hearing. We spend about $7 billion a year now on TSA's activities. And if anyone takes time to read this report—we're going to hear from John Roth in a few minutes, the inspector general who produced this report—but every Member of Congress and people throughout the country should read this report.

This report is an indictment of the failure of TSA, not just in one area, but in almost every one of their functions. It's supposed to be a multi-tiered transportation security system they set up; and in every aspect—just glance through the report—everything from passenger baggage screening and passenger screening, one indictment after another on systems to provide access for people who don't pose a risk, and we all support TSA PreCheck. They, in fact—and it's designed to expedite passengers who don't pose a risk. In fact, we find instances in which they failed to connect the dots and found a passenger who was a convicted terrorist, Sara Jane Olson—this is a press report—who went through TSA. Their system failed to find these people.

The most important thing we're trying to do is find people who pose a risk. The TSA agent who saw her go through actually identified her because she was such a well-known terrorist from her picture. And then what is even more astounding is he went to a superior, and he actually authorized the expediting of a terrorist through this system. This is an outrageous history.

And I have to say, the chairman is not Jason-come-lately. If you read further in the report, they talk about equipment purchases and the failure of buying. You have to have the best technology when someone comes through, not just an expedited system, but to see what they have that poses a risk, whether it's arms or now explosives and other devices that might harm us.

Back in 2009 the chairman introduced legislation to restrict the purchase of some equipment that actually didn't do the job, and this is a press account back then, and he was thwarted. They ended up buying equipment—read the report, an indictment of buying billions of dollars worth of equipment that failed. They bought puffers that failed. They bought this Rapiscan equipment. And it's interesting, the history of it is also interesting that Linda Daschle represented one company—people might be familiar with that name L–3, and then Rapiscan which the chairman had raised some questions about privacy issues and not using it.

They went ahead and spent—they split the contract, a half a billion dollar contract between the two competing lobbyists. A half a billion for the equipment is one thing. Then it cost another quarter of a billion per set of equipment to install this stuff. But this is an indictment of even the remaining equipment. The Rapiscan the chairman had raised questions about had to be taken out, had to be taken out. But then on top of that, this report says the equipment they have, they can't maintain. They don't know whether it works or not, and they don't have people properly trained to run the equipment.

This is a very sad day, and I can see why TSA did not want to show up today. They have 61,000 employees. They have 15,000 administrators because we have a cap of 46,000 screeners. And this whole report outlines in each area, training,recruitment, acquisition of equipment, how they've failed. I see why that seat is empty today and TSA would not show their face to this Committee today. I yield back.

Chairman CHAFFETZ. Thank the gentlemen.

Chairman CHAFFETZ. I now recognize the Ranking Member, Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman, and I do thank you for calling this very important hearing. The Transportation Security Administration has an incredibly challenging mission. It has to strike just the right balance between passenger safety and passenger convenience. Everyone who has been to an airport in the past 15 years can relate to the frustration of waiting in long lines at security checkpoints.

But after 9/11, we are painfully aware of the dangers we face on a continuing basis. The challenge of the TSA is to develop programs that maximize safety and convenience, programs that protect the traveling public without making their experience unbearable.

Last year Congress directed TSA to increase the number of passengers enrolled in the PreCheck program. Under the program, travelers submit background information, criminal histories and fingerprints. This information is run against terrorist watch lists and criminal data bases. If these searches turn up no problems, passengers are given known traveler numbers, and that allows them to pass through expedited security lines with fewer restrictions.

When Congress passed this law, it gave TSA specific targets. For example, Congress directed TSA to certify that 25 percent of all passengers are eligible for expedited screening without lowering security standards, and that the agency has been working toward that goal. But, however, the inspector general and the Government Accountability Office have raised concerns about this process. For example, the current program relies on passengers to provide information about any new criminal convictions or similar information after they have enrolled in the program. In other words, the system relies on passengers to self-update.

According to the inspector general, TSA should develop a system to conduct 24-hour recurrent vetting of PreCheck members against law enforcement and intelligence data bases. I know many people and many agencies have been working for years to do just that. I also understand how difficult it is to link various local State and Federal data systems. However, this may be one area in which our Committee can offer unique assistance, especially with our wide jurisdiction that cuts across all levels of government.

GAO and the inspector general have also raised concern with the Managed Inclusion program. Under this program TSA officers identify passengers that are not enrolled in the PreCheck program and direct them to pass through the PreCheck security lanes if they appear to be low risk. TSA uses behavioral detection officers to identify passengers with low risk indicators, such as children and the

elderly, and they also employ explosive trace detection and K–9 teams.

GAO reported that although TSA has tested the individual pieces of the Managed Inclusion program, it has not tested them as a whole system. In addition, the inspector general recommended that TSA halt the Managed Inclusion program until technology can be developed to connect terrorist watch lists to individual airport security checkpoints.

Another concern is perimeter security. One of our witnesses today, Mr. Rafi Ron, of the New Age Security Solutions, has flagged this as an issue that needs much more attention, particularly given the various entities that play a role in this process, including local airport police, airport operators, and TSA.

After a 15-year-old hopped a fence at the San Jose International Airport, climbed into an aircraft wheel well, and traveled to Hawaii, the Associated Press initiated the investigation of perimeter breaches. AP reported that approximately 268 perimeter security breaches have occurred since 2004 in airports that handle three-quarters of the Nation's commercial passenger traffic. We're better than that. We're only as strong as the weakest link in our chain, so it is important to ensure that all of these issues are addressed. It is easy to simply criticize the agency, but it is much more difficult, and it takes much more effort to identify solutions to these problems and ensure that they are well-implemented.

I want to thank Chairman Chaffetz for calling this hearing, and, Mr. Chairman, I agree; Mr. Carraway ought to be here. And as I said to you before the hearing began, we need to fix a date for him to come in so that we can hear from him. I know the chairman has focused on these issued extensively, and I want to thank him for all of his hard work in this area, and I also look forward to the testimony today; and with that I yield back.

Chairman CHAFFETZ. I thank the gentleman.

Chairman CHAFFETZ. I will hold the record open for 5 legislative days for any members who would like to submit a written Statement.

Chairman CHAFFETZ. But now will recognize our panel of witnesses. As I mentioned earlier, Mr. Melvin Carraway, Acting Administrator for the Department—of Transportation Security Administration at the Department of Homeland Security was scheduled to testify but has not arrived, has not shown up, has elected to not testify today, which was not an optional activity.

We are pleased to have the Honorable John Roth, Inspector General for the Department of Homeland Security; Ms. Jennifer Grover, Acting Director of Homeland Security and Justice at the Government Accountability Office; and Mr. Rafi Ron, President and CEO of New Age Security Solutions, who also has extensive airport security work that he has personally participated in, in Israel.

We welcome you all. Pursuant to Committee rules, all witnesses will be sworn before they testify, so if you will please rise and raise your right-hand.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Thank you. Let the record reflect that all witnesses answered in the affirmative. In order to allow time for discussion, we would appreciate it if you would limit your testimony to 5 minutes. Your entire written record will be obviously made a part of the record. We're pretty liberal on your verbal comments, but try to keep it close to 5. And we'll start with you, Mr. Roth. You're now recognized for 5 minutes.

## WITNESS STATEMENTS

### STATEMENT OF THE HONORABLE JOHN ROTH

Mr. ROTH. Chairman Chaffetz, Ranking Member Cummings, and members of the Committee, thank you for inviting me here to testify today about airport security issues. Each day TSA is required to screen about 1.8 million passengers and about 3 million carryon bags at 450 airports nationwide. TSA faces a classic asymmetric threat. It cannot afford to miss a single, genuine threat without potentially catastrophic consequences. A terrorist, on the other hand, only needs to get it right once. TSA's 50,000 transportation security officers spend long hours performing tedious tasks that require constant vigilance. Complacency can be a huge problem. Ensuring consistency across DHS' largest work force would challenge even the best of organizations. Unfortunately, although nearly 14 years have passed since TSA's inception, we remain deeply concerned about its ability to execute its mission.

Since 2004 we have published more than 115 audit and inspection reports about TSA's programs and operations. We have issued hundreds of recommendations to attempt to improve TSA's efficiency and effectiveness. We have conducted a series of covert penetration tests, essentially testing TSA's ability to stop us from bringing in simulated explosives and weapons through checkpoints, as well as testing whether we could enter secure areas through other means. Although the results of those tests are classified, and we would be happy to brief any Member or their staffs in a secure setting with regard to our specific findings, we identified vulnerabilities caused by human and technology-based failures.

We have audited and reported on TSA's acquisitions. Our audit reports show that TSA faces significant challenges in contracting for goods and services. Despite spending billions on aviation security technology, our testing of certain systems has revealed no resulting improvement.

We have examined the performance of TSA's work force, which is largely a function of who is hired and how they are trained and managed. Our audits have repeatedly found that human error, often a simple failure to follow protocol, poses significant transportation security vulnerabilities. We have looked at how TSA plans for, buys, deploys, and maintains its equipment and have found challenges at every step in the process. These weaknesses have real and negative impact on transportation security as well.

Additionally, we have looked at how TSA assesses risk in determining expedited screening. We applaud TSA's efforts to use risk-based passenger screening because it allows TSA to focus on high or unknown risk passengers instead of known, vetted passengers

who pose less risk. However, we have deep concerns about some of TSA's decisions about the level of risk.

We recently assessed the PreCheck Initiative. As a result of that inspection, we concluded that some of the methods that the TSA used in determining risk are sound approaches to increasing the PreCheck population. But other methods, specifically some of TSA's risk assessment rules, create security vulnerabilities. Based on our review, we believe TSA needs to modify the Initiative's vetting and screening processes. Unfortunately TSA did not concur with the majority of our recommendations. We believe that this represents TSA's failure to understand the gravity of the situation.

As an example of PreCheck's vulnerabilities, we recently reported that, through risk assessment rules, a notorious felon was granted expedited screening through PreCheck. The traveler was a former member of a domestic terrorist group and while a member was involved in numerous felonious criminal activities that led to arrest and conviction. After serving a multiple-year prison sentence, the traveler was released. Notwithstanding the fact that the transportation security officer recognized the traveler based on media coverage, that traveler was permitted to use expedited screening.

TSA has taken some steps to implement our recommendations and address security vulnerabilities. Nevertheless, some problems appear to persist. While TSA cannot control all risks to transportation security, many issues are well within their control. Sound planning and strategies for efficiently acquiring, using, and maintaining screening equipment that operates at full capacity to detect dangerous items, for example, would go a long way toward improving overall operations. Better training and better management of transportation security officers would help mitigate the effects of human error, which can never be eliminated but can be reduced. Taken together, TSA's focus on its management practices and its oversight of its technical assets and work force would help enhance security as well as customer service for air passengers.

Mr. Chairman, this concludes my prepared Statement. I welcome any questions you or other members of the Committee may have.

Chairman CHAFFETZ. Thank you. And thanks to you and your staff who spent a lot of time putting this information together. We do appreciate it.

[The prepared Statement of Mr. Roth follows:]

**STATEMENT OF JOHN ROTH**

**INSPECTOR GENERAL**

**U.S. DEPARTMENT OF HOMELAND SECURITY**

**BEFORE THE**

**COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM**

**U.S. HOUSE OF REPRESENTATIVES**

***CONCERNING***

**TRANSPORTATION SECURITY: ARE OUR AIRPORTS SAFE?**

**MAY 13, 2015**

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for inviting me here today to discuss airport security issues.

TSA's mission—to protect the Nation's transportation systems to ensure freedom of movement for people and commerce—is incredibly difficult. First, it is a massive operation, with a budget of more than $7.2 billion in fiscal year (FY) 2015. Each day, TSA screens about 1.8 million passengers and about 3 million carry-on bags at 450 airports nationwide. Second, we face a classic asymmetric threat in attempting to secure our transportation security: TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, yet a terrorist only needs to get it right once. TSA's 50,000 transportation security officers (TSO) spend long hours performing tedious tasks that require constant vigilance. Complacency can be a huge detriment to TSA's ability to carry out its mission. Ensuring consistency across DHS' largest workforce would challenge even the best organization.

Unfortunately, although nearly 14 years have passed since TSA's inception, we remain deeply concerned about its ability to execute its important mission. Since 2004, we have published more than 115 audit and inspection reports about TSA's programs and operations. We have issued hundreds of recommendations to attempt to improve TSA's efficiency and effectiveness.

- We have conducted a series of covert penetration tests—essentially testing TSA's ability to stop us from bringing simulated explosives and weapons through checkpoints, as well as testing whether we could enter secured areas through other means. Although the results of those tests are classified, we identified vulnerabilities caused by human and technology-based failures.

- We have audited and reported on TSA's acquisitions. Our audit results show that TSA faces significant challenges in contracting for goods and services. Despite spending billions on aviation security technology, our testing of certain systems has revealed no resulting improvement.

- We have examined the performance of TSA's workforce, which is largely a function of who is hired and how they are trained and managed. Our audits have repeatedly found that human error—often a simple failure to follow protocol—poses significant vulnerabilities.

- We have looked at how TSA plans for, buys, deploys, and maintains its equipment and have found challenges at every step in the process. These weaknesses have a real and negative impact on transportation security as well.

My testimony today will focus on the vulnerabilities and challenges identified by our more recent work on passenger and baggage screening, access controls to secured areas, workforce integrity, and TSA's operations.

**Passenger and Baggage Screening**

*Risk Assessment Rules*

We applaud TSA's efforts to use risk-based passenger screening because it allows TSA to focus on high- or unknown-risk passengers instead of known, vetted passengers who pose less risk to aviation security. However, we have deep concerns about some of TSA's decisions about this risk. For example, we recently assessed the PreCheck initiative, which is used at about 125 airports to identify low-risk passengers for expedited airport checkpoint screening.

Since 2012, TSA has massively increased the use of PreCheck, allowing expedited screening for nearly half of the flying public. TSA did so in four ways:

- Granted PreCheck eligibility to other Federal Government-vetted or known flying populations, such as those in the CBP Trusted Traveler Program.

- Established and increased the PreCheck application program, which requires individualized security threat assessment vetting.

- Implemented risk assessment rules.

- Used "managed inclusion" for the general public, allowing random passengers access to PreCheck lanes without having assessed their risk.

As a result of our inspection, we concluded that the first two methods are sound approaches to increasing the PreCheck population, but the latter two create security vulnerabilities. Based on our review, we believe TSA needs to modify the initiative's vetting and screening processes. We also determined that PreCheck communication and coordination need

improvement. TSA did not concur with the majority of our 17 recommendations; we believe this represents TSA's failure to understand the gravity of the situation. (*Security Enhancements Needed to the TSA PreCheck Initiative, (Unclassified Summary) OIG-15-29*)

As an example of PreCheck's vulnerabilities, we recently reported that, through risk assessment rules, a felon was granted expedited screening through PreCheck. The traveler was a former member of a domestic terrorist group and, while a member, was involved in numerous felonious criminal activities that led to arrest and conviction. After serving a multiple-year sentence, the traveler was released from prison.

The traveler was sufficiently notorious that a TSO recognized the traveler, based on media coverage. In scanning the traveler's boarding pass, the TSO received notification that the traveler was PreCheck eligible. The TSO, aware of the traveler's disqualifying criminal convictions, notified his supervisor who directed him to take no further action and allow the traveler to proceed through the PreCheck lane.

TSA agreed to modify its standard operating procedures to clarify TSOs' and supervisory TSOs' authority in referring passengers with PreCheck boarding passes to standard screening lanes when they believe it is warranted. However, TSA disagreed with our recommendation regarding the Secure Flight program. The failure to implement this recommendation perpetuates a security vulnerability. (*Allegation of Granting Expedited Screening through TSA PreCheck Improperly (Redacted) OIG-15-45*)

We are pleased to report that bipartisan legislation has been introduced to address this issue. The legislation, known as the *Securing Expedited Screening Act* (H.R. 2127), would direct the TSA to make expedited screening available only to individuals who are vetted PreCheck participants and to people TSA identifies as known-risk and low-risk, such as those enrolled in CBP's Global Entry program or other DHS trusted traveler programs. We support this legislation and believe it represents an important step forward in transportation security.

*Passenger and Baggage Screening*

Detection of dangerous items on people and in baggage requires reliable equipment with effective technology, as well as well-trained and alert TSOs who understand and consistently follow established procedures and exercise good judgment. We believe there are vulnerabilities in TSA's screening operations, caused by a combination of technology failures and human error. Since 2004, we have conducted eight covert penetration

testing audits on passenger and baggage screening operations. Because these audits involved covert testing and contain classified or Sensitive Security Information, we can only discuss the results in general terms at this hearing. However, we would be happy to schedule a private briefing with this Committee or staff to discuss the information we are not able to disclose today.

One penetration testing audit identified vulnerabilities in TSA's use of Advanced Imaging Technology (AIT) equipment[1] at domestic airports. TSA acknowledged that it could improve operation of new passenger screening technologies to prevent individuals with threat objects from entering airport secure areas undetected and agreed to take the necessary steps to increase AIT's effectiveness. (*TSA Penetration Testing of Advanced Imaging Technology (Unclassified Summary), OIG 12-06*)

In September 2014, we reported the classified results of our tests of checked baggage screening. We also reported that TSA did not have a process to assess the causes of equipment-based test failures or the capability to independently evaluate whether deployed explosive detection systems were operating at the correct detection standards. According to TSA, since 2009, it had spent $540 million for checked baggage screening equipment and $11 million for training. Despite that investment, TSA had not improved checked baggage screening since our 2009 report on the same issue. (*Vulnerabilities Exist in TSA's Checked Baggage Screening Operations (Unclassified Summary), OIG-14-142*)

We are currently conducting covert testing to evaluate the effectiveness of TSA's Automated Target Recognition software[2] and checkpoint screener performance in identifying and resolving potential security threats at airport checkpoints. Once that testing is completed and evaluated, we will report our results to the Secretary and Congress.

TSA uses layers of security to prevent dangerous items or individuals from entering aircraft. In one layer, TSA uses behavior detection officers to identify passenger behaviors that may indicate stress, fear, or deception. This program, Screening Passengers by Observation

---

[1] AIT equipment screens passengers for metallic and nonmetallic threats, including weapons, explosives, and other objects concealed under layers of clothing, without physical contact.

[2] Automated Target Recognition software is designed to enhance passenger privacy by eliminating passenger-specific images and instead auto-detecting potential threats and highlighting their location on a generic outline that is identical for all passengers.

Techniques (SPOT), includes more than 2,800 employees and has cost taxpayers about $878 million from FYs 2007 through 2012.

In 2013, we audited the SPOT program and found that TSA could not ensure that passengers were screened objectively. Nor could it show that the program was cost effective or merited expansion. Further, in a November 2013 report on the program, the Government Accountability Office (GAO) reported that TSA risked funding activities that had not been determined to be effective. Specifically, according to its analysis of more than 400 studies, GAO concluded that SPOT program behavioral indicators might not be effective in identifying people who might pose a risk to aviation security. TSA has taken steps to implement our recommendations and improve the program. However, the program remains an example of a questionable investment in security. (*Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted), OIG-13-91*)

**Access Controls to Secure Areas and Workforce Integrity**

Airport employees, as well as unauthorized individuals, entering the secure areas of airports, pose a serious potential risk to security. Controlling access to secured airport areas is critical to the safety of passengers and aircraft. Despite TSA's efforts to ensure only cleared individuals enter secure areas, we have identified numerous vulnerabilities.

*Airport Badges and Access to Secure Areas*

In February 2013, we identified problems with TSA's Aviation Channeling Services Provider project, which uses vendors to relay airport badge applicants' biographical information and fingerprints to TSA for vetting. Because TSA did not properly plan, manage, or implement the project, airports nationwide experienced a backlog of background checks. To address the backlog, TSA temporarily allowed airports to issue badges without the required background checks. Consequently, at least five airports granted badges to individuals with criminal records, giving them access to secure airport areas. In response to our findings, TSA agreed to develop a lessons learned report, establish a policy requiring all projects to include a comprehensive plan, communicate customer service expectations to vendors and monitor their performance for accountability, and require inspectors to review badges issued without the required background checks. (*Transportation Security Administration's Aviation Channeling Services Provider Project, OIG-13-42*)

We also used covert testing to determine whether unauthorized and potentially dangerous individuals could gain access to secured airport areas. In addition, during this audit, we identified the extent to which TSOs, airport employees, aircraft operators, and contractors were complying with related Federal aviation security requirements. Our test results are classified and cannot be discussed here today, but we can say that we identified significant access control vulnerabilities and recommended improvements. (*Covert Testing of Access Controls to Secured Airport Areas, OIG-12-26*)

In response to congressional concerns and media reports about missing badges, which could allow unauthorized people access to secure airport areas, we very recently began a review of TSA's controls over access badges. We intend to identify and test TSA's efforts to mitigate the risks of unaccounted for, lost, stolen, or terminated airport-issued badges.

Additionally, this month we will publish the final report from an audit we conducted of TSA's controls over the vetting of aviation workers possessing or applying for credentials that allow unescorted access to secure areas of commercial airports. Specifically, we assessed TSA's process for vetting workers for terrorist links, criminal history, and lawful status. We also sought to determine the accuracy and reliability of the data TSA uses for vetting.

*Workforce Integrity*

The integrity of TSA's workforce is also an important factor in the safety of our airports, as well as the public's trust in TSA's handling of their personal belongings. Although only a small percentage of TSA employees have committed crimes or engaged in other egregious misconduct, even a few publicized cases of wrongdoing can affect the public's confidence and potentially undermine deterrence.

Some of these crimes are serious. For example, we investigated a TSO who conspired with members of the public in a scheme to smuggle Brazilian nationals through an international airport. For his role in the crime, the TSO was sentenced to 10 months' incarceration, followed by 36 months of supervised release.

In another case, a supervisory TSO was convicted for assisting a drug trafficking organization responsible for smuggling large quantities of narcotics through an airport. With the supervisory TSO's assistance, the organization bypassed security with the narcotics and passed them to couriers on the secure side of the airport for transport to the United

States. The TSO was sentenced to 87 months of imprisonment and 2 years supervised release.

**TSA Operations and Management Oversight**

We have continuing concerns with TSA's stewardship of taxpayer dollars spent on aviation security.

*Acquiring and Maintaining Equipment*

Over the years, TSA has made significant investments in acquiring and maintaining passenger and baggage screening equipment, including Explosives Detection System machines, Explosives Trace Detection machines, AIT machines, Bottled Liquid Scanners, x-ray machines, and walkthrough metal detectors, yet a series of our audits found issues with TSA's acquisition management.

We conducted an audit of TSA's methods for planning, deploying, and using AIT machines at airports. We found that the component did not develop a comprehensive deployment strategy for this equipment. TSA also did not require program offices to prepare strategic acquisition or deployment plans for new technology that aligned with the overall needs and goals of its passenger screening program. As a result, despite spending approximately $150 million on AIT units, TSA continued to screen the majority of passengers with walkthrough metal detectors. Without documented, approved, comprehensive plans and accurate data on the use of AIT, TSA was unable to effectively deploy this new technology where it was needed and, instead, relied on walkthrough metal detectors to screen the majority of passengers. By doing so, TSA potentially reduced the technology's security benefits and may have inefficiently used resources to purchase and deploy the units. (*Transportation Security Administration's Deployment and Use of Advanced Imaging Technology, OIG-13-120*)

Another recent audit revealed that the safety of airline passengers and aircraft could be compromised by TSA's inadequate oversight of its equipment maintenance contracts. TSA has four maintenance contracts valued at about $1.2 billion, which cover both preventive and corrective maintenance for airport screening equipment. Because TSA does not adequately oversee equipment maintenance, it cannot be assured that routine preventive maintenance is performed on thousands of screening units or that this equipment is repaired as needed, ready for operational use, and operating at its full capacity. In response to our recommendations, TSA agreed to develop, implement, and enforce policies and procedures to ensure its screening equipment is maintained

as required and is fully operational while in service. (*The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program*, OIG-15-86)

*Use of Criminal Investigators*

Our report on TSA's Office of Inspection provides another example of TSA's lack of stewardship of taxpayer dollars. In September 2013, we reported that the Office of Inspection did not use its staff and resources efficiently to conduct cost-effective inspections, internal reviews, and covert testing. The office employed personnel classified as "criminal investigators," who received premium pay and other costly benefits, even though other employees were able to perform the same work at a substantially lower cost. Additionally, the office's quality controls were not sufficient to ensure that its work complied with accepted standards, that staff members were properly trained, and that its work was adequately reviewed. Finally, the office could not always ensure that other TSA components took action on its recommendations to improve TSA's operations. We estimated that TSA could save as much as $17.5 million in premium pay over 5 years by reclassifying criminal investigator positions to noncriminal investigator positions.

As a result of our efforts, in February of this year, the House passed the *TSA Office of Inspection Accountability Act* (H.R. 719). Among other things, this legislation requires TSA to reclassify criminal investigator positions in the Office of Inspection as noncriminal investigator positions if the individuals in those positions do not, or are not expected to, spend an average of at least 50 percent of their time performing criminal investigative duties. This legislation is now with the Senate Committee on Commerce, Science, and Transportation. (*Transportation Security Administration Office of Inspection's Efforts To Enhance Transportation Security*, OIG-13-123)

*Cybersecurity*

We have conducted a number of audits that highlight our concerns about TSA's management of its information technology (IT). During onsite inspections of IT systems, we found significant, repeated deficiencies in IT systems that support TSA's operations. These include insufficient physical security and access controls for numerous TSA server rooms and communication closets, failure to implement known software patches to servers, and other deviations from DHS IT policies and procedures. Collectively, these deficiencies place the confidentiality, integrity, and availability of TSA's data at risk. We are especially concerned that repeated deficiencies mean lessons learned at one airport

are not being shared with other airports. (*Audit of Security Controls for DHS Information Systems at John F. Kennedy International Airport (Redacted) (Revised), OIG-15-18; Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport, OIG-14-132; Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport, OIG-13-104*)

This month, we will begin an audit to determine whether TSA has incorporated adequate IT security controls to ensure that its Security Technology Integrated Program (STIP) equipment performs effectively and efficiently. STIP combines various technologies to perform passenger and baggage screening. Transportation security equipment includes the servers, databases, storage devices, and systems used for explosives detection, explosive trace detection, advanced X-ray and imaging, and credential authentication. We expect to publish our final report on STIP security around the end of this year.

**Conclusion**

TSA has taken some steps to implement our recommendations and address security vulnerabilities. Nevertheless, some problems appear to persist. TSA cannot control all risks to transportation security and unexpected threats will arise that will require TSA to improvise, but other issues are well within TSA's control. Sound planning and strategies for efficiently acquiring, using, and maintaining screening equipment that operates at full capacity to detect dangerous items, for example, would go a long way toward improving overall operations. Better training and better management of TSOs would help mitigate the effects of human error that, although never eliminated, can be reduced. Taken together, TSA's focus on its management practices and oversight of its technical assets and its workforce would help enhance security, as well as customer service, for air passengers.

Mr. Chairman, this concludes my prepared statement. I welcome any questions you or other Members of the Committee may have.

**Appendix**

OIG Reports Referenced in This Testimony

*Security Enhancements Needed to the TSA PreCheck™ Initiative (Redacted)*, OIG-15-29, January 2015

*Allegation of Granting Expedited Screening through TSA PreCheck Improperly (OSC File NO. DI-14-3679)*, OIG-15-45, March 2015

*TSA Penetration Testing of Advanced Imaging Technology (Unclassified Summary), OIG 12-06, November 2011*

*Vulnerabilities Exist in TSA's Checked Baggage Screening Operations (Unclassified Summary)*, OIG-14-142, September 2014

*Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted)*, OIG-13-91, May 2013

*Transportation Security Administration's Aviation Channeling Services Provider Project*, OIG-13-42, February 2013

*Covert Testing of Access Controls to Secured Airport Areas (Unclassified Summary)*, OIG-12-26, January 2012

*Transportation Security Administration's Deployment and Use of Advanced Imaging Technology*, OIG-13-120, March 2014

*The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program*, OIG-15-86, May 2015

*Transportation Security Administration Office of Inspection's Efforts To Enhance Transportation Security*, OIG-13-123, September 2013

*Audit of Security Controls for DHS Information at John F. Kennedy International Airport (Redacted) (Revised)*, OIG-15-18, January 16, 2015

*Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport*, OIG-14-132, September 2014

*Technical Security Evaluation of DHS Activities at Hartsfield Jackson Atlanta International Airport*, OIG-13-104, July 2013

Chairman CHAFFETZ. Ms. Grover. You're recognized for 5 minutes.

**STATEMENT OF JENNIFER GROVER**

Ms. GROVER. Good morning, Chairman Chaffetz, Ranking Member Cummings, and other members and staff. Thank you for the opportunity to discuss TSA's oversight of passenger and airport worker screening effectiveness.

Screening systems must work properly to deliver the security protections that they promise. Over several years GAO has found weaknesses in TSA's oversight of its screening systems, raising questions about whether TSA is falling short in its ability to ensure aviation security. TSA has taken some steps to improve oversight of these systems, but additional actions are needed.

Today I will focus on four areas. First, a Secure Flight program which matches passenger information against Federal Government watch lists to ensure that those who should not fly or should receive enhanced screening are identified. Second, AIT systems, which are the full body scanners that are used to screen passengers for prohibited items at the checkpoint. Third, the Managed Inclusion screening process which TSA uses to provide expedited screening to passengers who were not previously identified as low risk; and, fourth, criminal history checks done to vet airport workers.

Regarding Secure Flight, we found in September 2014 that TSA did not have timely and reliable information about the extent or causes of system matching errors which occur when Secure Flight fails to identify passengers who were actual matches to the watch list. In response to our recommendation, TSA has developed a mechanism to keep track of the known matching errors, and they are considering methods to evaluate overall Secure Flight matching accuracy rates on an ongoing basis.

Regarding AIT, we found in March 2014, that TSA did not include information about screener performance when they were evaluating AIT effectiveness. Rather, TSA's assessment was limited to the accuracy of the AIT systems in the laboratory. However, after an AIT identifies a potential threat, a screening officer must do a targeted pat down to resolve the alarm. Thus, the accuracy of the screeners in conducting their pat downs properly and identifying all threat items is key to understanding the effectiveness of the AIT systems in the airport operating environment.

DHS concurred with our recommendation to measure AIT effectiveness as a function of both the technology and the screening officers who operate it but has not yet fully addressed the recommendation.

Similarly, in December 2014, we found that TSA had not tested the security effectiveness of the Managed Inclusion system as it functions as a whole. As part of Managed Inclusion, TSA uses multiple layers of security, as you noted in your opening Statements, such as explosive detection devices and canines, to mitigate the inherent risk that's associated with screening randomly selected passengers in a system that was specifically designed for low-risk passengers. However, if the security layers are not working as intended, then TSA may not be sufficiently screening passengers. As you noted, TSA has tested the individual layers of security used in

Managed Inclusion and has reported finding them effective, although GAO has raised concerns about the effectiveness of some of these layers such as behavior detection officers. At the time of our report, TSA was planning to complete testing of the Managed Inclusion system by mid–2016.

Finally, regarding TSA's involvement in airport worker vetting, we found in December 2011 that the criminal history information available to TSA and airports for background checks was limited. Specifically, TSA's level of access to FBI criminal history records was excluding many State records. In response to our recommendation, TSA and the FBI confirmed that there was a risk of incomplete information, and the FBI has since reported expanding the criminal history records information that is available to TSA for these security threat assessments.

In conclusion, TSA has made progress in improving its screening oversight such as by taking steps to understand the vulnerabilities in the Secure Flight program, and by working with the FBI to obtain access to more complete criminal background information. Yet more work remains to ensure that Secure Flight, AIT, and Managed Inclusion are working as TSA intends.

Chairman Chaffetz, Ranking Member Cummings, this concludes my Statement. I look forward to your questions.

Chairman CHAFFETZ. Thank you.

[Prepared Statement of Ms. Grover follows:]

United States Government Accountability Office

GAO

Testimony
Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00a.m ET
Wednesday, May 13, 2015

# AVIATION SECURITY

# TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed

Statement of Jennifer Grover, Director, Homeland Security and Justice

May 13, 2015

# GAO Highlights

Highlights of GAO-15-559T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

# AVIATION SECURITY

## TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed

### Why GAO Did This Study

Since the attacks of September 11, 2001 exposed vulnerabilities in the nation's aviation system, billions of dollars have been spent on a wide range of programs designed to enhance aviation security. Securing commercial aviation remains a daunting task, and continuing fiscal pressure highlights the need for TSA to determine how to allocate its finite resources for the greatest impact. GAO previously reported on TSA's oversight of its aviation security programs, including the extent to which TSA has the information needed to assess the programs.

This testimony focuses on TSA's oversight of aviation security measures including, among other things (1) Secure Flight, (2) Advanced Imaging Technology, and (3) Managed Inclusion. This statement is based on reports and testimonies issued from December 2011 through March 2015, with selected updates conducted from November 2014 through April 2015 to determine progress made in implementing previous GAO recommendations. For prior work, GAO analyzed TSA documents and interviewed TSA officials, among other things. For the updates, GAO reviewed documents and interviewed TSA officials about actions taken to address our recommendations.

### What GAO Recommends

GAO has previously made recommendations to DHS to strengthen TSA's oversight of aviation security programs. DHS generally agreed and has actions underway to address them. Consequently, GAO is not making any new recommendations in this testimony.

View GAO-15-559T. For more information, contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov.

### What GAO Found

The Transportation Security Administration (TSA) has taken steps to improve oversight of Secure Flight—a passenger prescreening program that matches passenger information against watch lists to assign each passenger a risk category—but could take further action to address screening errors. In September 2014, GAO reported that TSA lacked timely and reliable information on system matching errors—instances where Secure Flight did not identify passengers who were actual matches to watch lists. GAO recommended that TSA systematically document such errors to help TSA determine if actions can be taken to prevent similar errors from occurring. The Department of Homeland Security (DHS) concurred and has developed a mechanism to do so, but has not yet shown how it will use this information to improve system performance. In September 2014, GAO also found that screening personnel made errors in screening passengers at the checkpoint at a level consistent with their Secure Flight risk determinations and that TSA did not have a systematic process for evaluating the root causes of these errors across airports. GAO recommended that TSA develop a process for evaluating the root causes and implement corrective measures to address them. DHS concurred and has developed such a process but has not yet demonstrated implementation of corrective measures.

In March 2014, GAO found that TSA performance assessments of certain full-body scanners used to screen passengers at airports did not account for all factors affecting the systems. GAO reported that the effectiveness of Advanced Imaging Technology (AIT) systems equipped with automated target recognition software (AIT-ATR)—which displays anomalies on a generic passenger outline instead of actual passenger bodies—relied on both the technology's capability to identify potential threat items and its operators' ability to resolve them. However, GAO found that TSA did not include these factors in determining overall AIT-ATR system performance. GAO also found that TSA evaluated the technology's performance in the laboratory—a practice that does not reflect how well the technology will perform with actual human operators. In considering procurement of the next generation of AIT systems (AIT-2), GAO recommended that TSA measure system effectiveness based on the performance of both the technology and the screening personnel. DHS concurred and in January 2015 reported that it has evaluated the AIT-2 technology and screening personnel as a system but has not yet provided sufficient documentation of this effort.

In December 2014, GAO found that TSA had not tested the effectiveness of its overall Managed Inclusion process—a process to assess passenger risk in real time at the airport and provide expedited screening to certain passengers—but had plans to do so. Specifically, GAO found that TSA had tested the effectiveness of individual components of the Managed Inclusion process, such as canine teams, but had not yet tested the effectiveness of the overall process. TSA officials stated that they had plans to conduct such testing. Given that GAO has previously reported on TSA challenges testing the effectiveness of its security programs, GAO recommended that TSA ensure its planned testing of the Managed Inclusion process adhere to established evaluation design practices. DHS concurred and has plans to use a test and evaluation process for its planned testing of Managed Inclusion.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

I am pleased to be here today to discuss our past work examining the Transportation Security Administration's (TSA) oversight of its passenger and airport worker screening programs. It has been nearly 14 years since the attacks of September 11, 2001 exposed vulnerabilities in the nation's aviation system. Since then, billions of dollars have been spent on a wide range of programs designed to enhance aviation security. However, securing commercial aviation operations remains a daunting task—with hundreds of airports, thousands of aircraft, and thousands of flights daily carrying millions of passengers and pieces of carry-on and checked baggage. According to TSA, the threat to civil aviation has not diminished—underscoring the need for effective passenger and airport worker screening programs. As the fiscal pressures facing the government continue, so too does the need for TSA to determine how to allocate its finite resources to have the greatest impact on addressing threats and strengthening the effectiveness of its programs and activities. GAO previously reported on TSA's oversight of its aviation security programs, including the extent to which TSA has the information needed to assess the programs.

As requested, my testimony today focuses on TSA's oversight of four key aviation security measures:

- Secure Flight: a passenger prescreening program that matches passenger information against federal government watch lists and other information to assign each passenger to a risk category;
- Advanced Imaging Technology (AIT): a full body scanner used to screen passengers in the nation's airports;
- Managed Inclusion process: a process that TSA uses to determine passengers' eligibility for expedited screening at some passenger screening checkpoints, via Pre✓™ lanes;[1] and

[1]TSA Pre✓™ is the program through which TSA designates passengers as low risk for expedited screening in advance of their arrival at the passenger screening checkpoint. Expedited screening typically includes walk-through metal detector screening and X-ray screening of the passenger's accessible property, but unlike in standard screening, travelers do not have to, among other things, remove their belts, shoes, or light outerwear. Managed Inclusion operates only at checkpoints with TSA Pre✓™ lanes.

- Aviation Workers: a program by which TSA and airports, in collaboration with the Federal Bureau of Investigation (FBI), vet applicants against the FBI's criminal history records, among other databases, and issue credentials to qualifying airport facility workers, retail employees, and airline employees, among others.

This statement is based on our reports and testimonies issued from December 2011 through March 2015 related to TSA's efforts to oversee its aviation security measures. In addition, this statement is based on selected updates conducted from November 2014 through April 2015 related to the current status of the Secure Flight, AIT, Managed Inclusion, and Aviation Workers programs and progress made in implementing previous GAO recommendations. For our past work, we reviewed applicable laws, regulations, and policies as well as TSA program documents; results from AIT testing and screener performance reviews; decision memorandums; and other documents. We also visited airports—six for our Managed Inclusion work and nine for our Secure Flight work—which we selected based on a variety of factors, such as volume of passengers screened and geographic dispersion, and interviewed Department of Homeland Security (DHS), TSA, FBI officials, among other things. Further details on the scope and methodology for the previously issued reports and testimonies are available within each of the published products. For the updates, we reviewed documents and interviewed TSA officials related to the actions taken to address our recommendations. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Background

The Aviation and Transportation Security Act (ATSA) established TSA as the primary federal agency with responsibility for securing the nation's civil aviation system.[2] This responsibility includes the screening of all passengers and property transported from and within the United States

[2]Pub. L. No. 107-71, 115 Stat. 597 (2001).

by commercial passenger aircraft.[3] In accordance with ATSA, all passengers, their accessible property, and their checked baggage are screened pursuant to TSA-established procedures at the more than 450 airports at which TSA performs, or oversees the performance of, security screening operations. These procedures generally provide, among other things, that passengers pass through security checkpoints where their person, identification documents, and accessible property, are checked by screening personnel.[4]

## Secure Flight

Since its implementation, in 2009, Secure Flight has changed from a program that identifies passengers as high risk solely by matching them against federal government watch lists—primarily the No Fly List, comprised of individuals who should be precluded from boarding an aircraft, and the Selectee List, composed of individuals who should receive enhanced screening at the passenger security checkpoint—to one that uses additional lists and risk-based criteria to assign passengers to a risk category: high risk, low risk, or unknown risk.[5] In 2010, following the December 2009 attempted attack on a U.S.-bound flight, which exposed gaps in how agencies used watch lists to screen individuals, TSA began using risk-based criteria to create additional lists for Secure Flight screening. These lists are composed of high-risk passengers who may not be in the Terrorist Screening Database (TSDB), but who TSA

[3]See 49 U.S.C. § 44901. For purposes of this testimony, "commercial passenger aircraft" refers to U.S.- or foreign-flagged air carriers operating under TSA-approved security programs with regularly scheduled passenger operations to or from a U.S. airport. "Commercial aviation," as the term is used in this testimony, encompasses the transport of passengers and their property by commercial passenger aircraft as well as the airports that service such aircraft.

[4]Screening personnel include transportation security officers, and at airports participating in TSA's Screening Partnership Program, screeners employed by private companies perform this function under contract with and overseen by TSA. See 49 U.S.C. §§ 44901, 44920.

[5]The No Fly and Selectee Lists are subsets of the Terrorist Screening Database—the U.S. government's consolidated watch list of known or suspected terrorists.

has determined should be subject to enhanced screening procedures.[6] Further, in 2011, TSA began screening passengers against additional identities in the TSDB that are not included on the No Fly or Selectee Lists. In addition, as part of TSA Pre✓™, a 2011 program through which TSA designates passengers as low risk for expedited screening, TSA began screening against several new lists of preapproved low-risk travelers. TSA also began conducting TSA Pre✓™ risk assessments, an activity distinct from matching against lists that uses the Secure Flight system to assign passengers scores based upon their travel-related data, for the purpose of identifying them as low risk for a specific flight.

## AIT Systems

According to TSA officials, AIT systems, also referred to as full-body scanners, provide enhanced security benefits compared with those of walk-through metal detectors by identifying nonmetallic objects and liquids. Following the deployment of AIT, the public and others raised privacy concerns because AIT systems produced images of passengers' bodies that image operators analyzed to identify objects or anomalies that could pose a threat to an aircraft or to the traveling public. To mitigate those concerns, TSA began installing automated target recognition (ATR) software on deployed AIT systems in July 2011.[7] AIT systems equipped with ATR (AIT-ATR) automatically interpret the image and display anomalies on a generic outline of a passenger instead of displaying images of actual passenger bodies. Screening officers use the generic image of a passenger to identify and resolve anomalies on-site in the presence of the passenger.

## TSA's Managed Inclusion Process

TSA Pre✓™ is intended to allow TSA to devote more time and resources at the airport to screening the passengers TSA determined to be higher or unknown risk, while providing expedited screening to those passengers

[6]Standard screening typically includes passing through a walk-through metal detector or Advanced Imaging Technology system, which identifies objects or anomalies on the outside of the body, and X-ray screening for the passenger's accessible property. In general, enhanced screening includes, in addition to the procedures applied during a typical standard screening experience, a pat-down and an explosives trace detection or physical search of the interior of the passenger's accessible property, electronics, and footwear.

[7]See Pub. L. No. 112-95, § 826, 126 Stat. 11, 132-33 (2012) (codified at 49 U.S.C. § 44901(*l*)) (requiring, in general, that TSA ensure that all AIT systems used to screen passengers are equipped with ATR software).

determined to pose a lower risk to the aviation system. To assess whether a passenger is eligible for expedited screening, TSA considers, in general, (1) inclusion on an approved TSA Pre✓™ list of known travelers;[8] (2) results from the automated TSA Pre✓™ risk assessments of all passengers;[9] and (3) real-time threat assessments of passengers, known as Managed Inclusion, conducted at airport checkpoints. Managed Inclusion uses several layers of security, including procedures that randomly select passengers for expedited screening and a combination of behavior detection officers (BDO), who observe passengers to identify high-risk behaviors at TSA-regulated airports; passenger-screening canine teams; and explosives trace detection (ETD) devices to help ensure that passengers selected for expedited screening have not handled explosive material.

## Aviation Workers Program

TSA also shares responsibility with airports to vet airport workers to ensure they do not pose a security threat. Pursuant to TSA's Aviation Workers program, TSA, in collaboration with airport operators and FBI, is to complete applicant background checks—known as security threat assessments—for airport facility workers, retail employees, and airline employees who apply for or are issued a credential for unescorted access to secure areas in U.S. airports.[10]

[8]These lists are composed of individuals whom TSA has determined to be low risk by virtue of their membership in a specific group, such as active duty military members, or based on group vetting requirements.

[9]Using these assessments, an activity distinct from watch list matching that uses the Secure Flight system to assign passengers scores based upon their travel-related data, TSA assigns passengers scores based upon information available to TSA to identify low-risk passengers eligible for expedited screening for a specific flight prior to the passengers' arrival at the airport.

[10]TSA security threat assessments include a background check to determine whether an applicant is a security risk to the United States. In general, security threat assessments include checks for criminal history records and immigration status, checks against terrorism databases and watch lists, and checks for records indicating an adjudication of lack of mental capacity, among other things. For airport workers, TSA is responsible for both vetting and adjudicating an applicant's terrorist and immigration history while providing the results of criminal history checks to airport operators. The airport operator is responsible for adjudicating the criminal history which includes a determination of whether an applicant has committed a disqualifying criminal offense, before determining whether to issue an applicant a credential for unescorted access to secure areas of the airport. See, e.g., 49 C.F.R. §§ 1542.209, 1544.229, & 1544.230 (listing or referencing disqualifying criminal offenses).

## TSA Has Taken Steps to Improve Oversight of Secure Flight, but Could Take Further Action to Measure Program Performance and Address Screening Errors

In September 2014, we reported on three issues affecting the effectiveness of TSA's Secure Flight program—(1) the need for additional performance measures to capture progress toward Secure Flight program goals, (2) Secure Flight system matching errors, and (3) mistakes screening personnel have made in implementing Secure Flight at the screening checkpoint.[11] TSA has taken steps to address these issues but additional action would improve the agency's oversight of the Secure Flight program.

**Need for additional performance measures:** In September 2014, we found that Secure Flight had established program goals that reflect new program functions since 2009 to identify additional types of high-risk and also low-risk passengers; however, the program performance measures in place at that time did not allow TSA to fully assess its progress toward achieving all of its goals. For example, one program goal was to accurately identify passengers on various watch lists. To assess performance toward this goal, Secure Flight collected various types of data, including the number of passengers TSA identifies as matches to high- and low-risk lists, but did not have measures to assess the extent of system matching errors—for example, the extent to which Secure Flight is missing passengers who are actual matches to these lists. We concluded that additional measures that address key performance aspects related to program goals, and that clearly identify the activities necessary to achieve goals, in accordance with the Government Performance and Results Act, would allow TSA to more fully assess progress toward its goals. Therefore, we recommended that TSA develop such measures, and ensure these measures clearly identify the activities necessary to achieve progress toward the goal. DHS concurred with our recommendation and, according to TSA officials, as of April 2015, TSA's Office of Intelligence and Analysis was evaluating its current Secure Flight performance goals and measures and determining what new performance measures should be established to fully measure progress against program goals.

**Secure Flight system matching errors:** In September 2014, we found that TSA lacked timely and reliable information on all known cases of Secure Flight system matching errors, meaning instances where Secure Flight did not identify passengers who were actual matches to these lists. TSA officials told us at the time of our review that when TSA receives

[11]GAO, *Secure Flight: TSA Should Take Additional Steps to Determine Program Effectiveness*, GAO-14-531 (Washington, D.C.: Sept. 9, 2014).

information related to matching errors of the Secure Flight system, the Secure Flight Match Review Board reviews this information to determine if any actions could be taken to prevent similar errors from happening again.[12] We identified instances in which the Match Review Board discussed system matching errors, investigated possible actions to address these errors, and implemented changes to strengthen system performance. However, we also found that TSA did not have readily available or complete information on the extent and causes of system matching errors. We recommended that TSA develop a mechanism to systematically document the number and causes of the Secure Flight system's matching errors, in accordance with federal internal control standards. DHS concurred with our recommendation, and as of April 2015, TSA had developed such a mechanism. However, TSA has not yet demonstrated how it will use the information to improve the performance of the Secure Flight system.

**Mistakes at screening checkpoint:** We also found in September 2014 that TSA had processes in place to implement Secure Flight screening determinations at airport checkpoints, but could take steps to enhance these processes. Screening personnel at passenger screening checkpoints are primarily responsible for ensuring that passengers receive a level of screening that corresponds to the level of risk determined by Secure Flight by verifying passengers' identities and identifying passengers' screening designations. To carry out this responsibility, among other steps, screening personnel are to confirm that the data included on the passenger's boarding pass and in his or her identity document (such as a driver's license) match one another, and review the passenger's boarding pass to identify his or her Secure Flight passenger screening determination. TSA information from May 2012 through February 2014 that we assessed indicates that screening personnel made errors at the checkpoint in screening passengers consistent with their Secure Flight determinations. TSA officials at five of the nine airports where we conducted interviews stated they conducted after-action reviews of such screening errors and used these reviews to take action to address the root causes of those errors. However, we found that TSA did not have a systematic process for evaluating the root causes of these screening errors across airports, which could allow TSA

[12]Secure Flight's Match Review Board—a multidepartmental entity—and associated Match Review Working Group review performance measurement results and recommend changes to improve system performance, among other things.

to identify trends across airports and target nationwide efforts to address these issues.

Officials with TSA's Office of Security Operations told us in the course of our September 2014 review that evaluating the root causes of screening errors would be helpful and stated they were in the early stages of forming a group to discuss these errors. However, TSA was not able to provide documentation of the group's membership, purpose, goals, time frames, or methodology. Therefore, we recommended in September 2014 that TSA develop a process for evaluating the root causes of screening errors at the checkpoint and then implement corrective measures to address those causes. DHS concurred with our recommendations and has developed a process for collecting and evaluating data on the root causes of screening errors. However, as of April 2015, TSA had not yet shown that the agency has implemented corrective measures to address the root causes.

## TSA Performance Assessments of AIT-ATR Did Not Account for All Factors Affecting the System

In March 2014, we reported that, according to TSA officials, checkpoint security is a function of technology, people, and the processes that govern them, however we found that TSA did not include each of those factors in determining overall AIT-ATR system performance.[13] Specifically, we found that TSA evaluated the technology's performance in the laboratory to determine system effectiveness. However, laboratory test results provide important insights but do not accurately reflect how well the technology will perform in the field with actual human operators. Additionally, we found that TSA did not assess how alarms are resolved by considering how the technology, people, and processes function collectively as an entire system when determining AIT-ATR system performance. AIT-ATR system effectiveness relies on both the technology's capability to identify threat items and its operators to resolve those threat items.

At the time of our review, TSA officials agreed that it is important to analyze performance by including an evaluation of the technology, operators, and processes, and stated that TSA was planning to assess the performance of all layers of security. According to TSA, the agency conducted operational tests on the AIT-ATR system, as well as follow-on operational tests as requested by DHS's Director of Operational Test and

[13]GAO, *Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems*, GAO-14-357 (Washington, D.C.: Mar. 31, 2014).

Evaluation, but those tests were not ultimately used to assess effectiveness of the operators' ability to resolve alarms, as stated in DHS's Director of Operational Test and Evaluation's letter of assessment on the technology. Transportation Security Laboratory officials also agreed that qualification testing conducted in a laboratory setting is not always predictive of actual performance at detecting threat items. Further, laboratory testing does not evaluate the performance of screening officers in resolving anomalies identified by the AIT-ATR system or TSA's current processes or deployment strategies.

Given that TSA was seeking to procure the second generation of AIT systems, known as AIT-2, we reported that DHS and TSA would be hampered in their ability to ensure that future AIT systems meet mission needs and perform as intended at airports unless TSA evaluated system effectiveness based on both the performance of the AIT-2 technology and screening officers who operate the technology. We recommended that TSA measure system effectiveness based on the performance of the AIT-2 technology and screening officers who operate the technology while taking into account current processes and deployment strategies. TSA concurred and reported taking steps to address this recommendation. Specifically, in January 2015, DHS stated that TSA's Office of Security Capabilities evaluated the AIT-2 technology and screening officer as a system during an operational evaluation. However, TSA has not yet provided sufficient documentation showing that this recommendation has been fully addressed.

## TSA Has Not Tested the Overall Effectiveness of Its Managed Inclusion Process, But Plans to Conduct Such Testing

In December 2014, we reported that, according to TSA officials, TSA tested the security effectiveness of the individual components of the Managed Inclusion process—such as BDOs and ETD devices—before implementing Managed Inclusion, and TSA determined that each layer alone provides an effective level of security.[14] However, in our prior body of work, we identified challenges in several of the layers used in the Managed Inclusion process, raising questions regarding their effectiveness.[15] For example, in our November 2013 report on TSA's behavior detection and analysis program, we found that although TSA had taken several positive steps to validate the scientific basis and strengthen program management of its behavior detection and analysis program, TSA had not demonstrated that behavioral indicators can be used to reliably and effectively identify passengers who may pose a threat to aviation security.[16]

Further, TSA officials stated that they had not yet tested the security effectiveness of the Managed Inclusion process as it functions as a whole, as TSA had been planning for such testing over the course of the last year. TSA documentation showed that the Office of Security Capabilities recommended in January 2013 that TSA test the security effectiveness of Managed Inclusion as a system. We reported in December 2014 that according to officials, TSA anticipated that testing would begin in October 2014 and estimated that testing could take 12 to 18 months to complete.

We have also previously reported on challenges TSA has faced in designing studies and protocols to test the effectiveness of security systems and programs in accordance with established methodological practices, such as in the case of the AIT systems discussed previously

[14]GAO, *Aviation Security: Rapid Growth in Expedited Passenger Screening Highlights Need to Plan Effective Security Assessments*, GAO-15-150 (Washington, D.C.: Dec. 12, 2014).

[15]See, GAO, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159 (Washington, D.C.: Nov. 8, 2013); *Explosives Detection Canines: TSA Has Taken Steps to Analyze Canine Team Data and Assess the Effectiveness of Passenger Screening Canines*, GAO-14-695T (Washington, D.C.: June 24, 2014); and *Aviation Security: TSA Has Enhanced Its Explosives Detection Requirements for Checked Baggage, but Additional Screening Actions Are Needed*, GAO-11-740 (Washington, D.C.: July 11, 2011).

[16]GAO-14-159.

and in our evaluation of BDO effectiveness.[17] In our December 2014 report, we concluded that ensuring the planned effectiveness testing of the Managed Inclusion process adheres to established evaluation design practices would help TSA provide reasonable assurance that the effectiveness testing will yield reliable results.[18] In general, evaluations are most likely to be successful when key steps are addressed during design, including defining research questions appropriate to the scope of the evaluation, and selecting appropriate measures and study approaches that will permit valid conclusions. As a result, we recommended that to ensure TSA's planned testing yields reliable results, the TSA Administrator take steps to ensure that TSA's planned effectiveness testing of the Managed Inclusion process adheres to established evaluation design practices. DHS concurred with our recommendation and began taking steps toward this goal. Specifically, DHS stated that TSA plans to use a test and evaluation process—which calls for the preparation of test and evaluation framework documents including plans, analyses, and a final report describing the test results—for its planned effectiveness testing of Managed Inclusion.

[17]In November 2013, we reported on methodological weaknesses in the overall design and data collection of TSA's April 2011 validation comparison study to determine the effectiveness of the behavior detection and analysis program. For example, we found that TSA had not randomly selected airports to participate in the study, so the results were not generalizable across airports. We recommended that future funding for the program be limited until TSA provided scientifically validated evidence that demonstrates that behavioral indicators can be used to identify passengers who may pose a threat to aviation security. See GAO-14-159.

[18]GAO, *Designing Evaluations: 2012 Revision*, GAO-12-208G (Washington, D.C.: January 2012).

## TSA and the FBI Have Addressed a Weakness in TSA's Oversight of Credentials for Airport Workers

In December 2011, we found that, according to TSA, limitations in its criminal history checks increased the risk that the agency was not detecting potentially disqualifying criminal offenses as part of its Aviation Workers security threat assessments for airport workers.[19] Specifically, we reported that TSA's level of access to criminal history record information in the FBI's Interstate Identification Index excluded access to many state records such as information regarding sentencing, release dates, and probation or parole violations, among others.[20] As a result, TSA reported that its ability to look into applicant criminal history records was often incomplete.

We recommended that the TSA and the FBI jointly assess the extent to which this limitation may pose a security risk, identify alternatives to address any risks, and assess the costs and benefits of pursuing each alternative. TSA and the FBI have since taken steps to address this recommendation. For example, in 2014, the agencies evaluated the extent of any risk and, according to TSA and FBI officials, concluded that the risk of incomplete information did exist and could be mitigated through expanded access to state-supplied records. TSA officials reported that the FBI has since taken steps to expand the criminal history record information available to TSA when conducting its security threat assessments for airport workers and others.

[19]GAO, *Transportation Security: Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload*, GAO-12-60 (Washington, D.C.: Dec. 8, 2011).

[20]The FBI's criminal history records contain information from a national fingerprint and criminal history system that responds to requests from local, state, and federal agencies. The system provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses. A segment of this system is the FBI-maintained criminal history record repository, known as the Interstate Identification Index (III, or Triple I) system that contains records from all states and territories, as well as from federal and international criminal justice agencies. The state records in the III are submitted to the FBI by central criminal record repositories that aggregate criminal records submitted by most or all of the local criminal justice agencies in their jurisdictions. The FBI's criminal history records check is a negative identification check, whereby the fingerprints are used to confirm that the associated individual is not identified as having a criminal record in the database. If an individual has a criminal record in the database, the FBI provides criminal history record check results to TSA. TSA, in turn transmits the results to the airport operator that, consistent with TSA regulations, is responsible for adjudicating the criminal history to identify potentially disqualifying criminal offenses and making a final determination of eligibility for a credential. See 49 C.F.R. § 1542.209.

Chairman Chaffetz, Ranking Member Cummings, and members of the committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

For questions about this statement, please contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Maria Strudwick (Assistant Director), Claudia Becker, Juli Digate, Michele Fejfar, Susan Hsu, and Tom Lombardi. Key contributors for the previous work that this testimony is based on are listed in each product.

Chairman CHAFFETZ. Mr. Ron, you are now recognized for 5 minutes.

**STATEMENT OF RAFI RON**

Mr. RON. First of all, I would like to thank the chairman and the members of the Committee for inviting me to testify again before you. I have chosen to speak today not on passenger screening, as the other witnesses have referred to this in details, but rather go into what Mr. Cummings mentioned earlier, and that is the failure to deal with what I would describe as the airport facility security, which is an extremely important part of our airport and aviation security system.

What I wish the Committee to understand is that the importance of perimeter security has to be measured against the threat of somebody being able to access an aircraft parked on the ground without knowledge, without detection. And in the case of a stowaway, as we have witnessed in the past, they tried to get—to take hide in the wheel well, but instead of that, certainly instead of 120 pounds of bone and flesh of a person, they leave behind a 2-pound device that will not be noticed.

The measures that are being implemented today are simply unable to do that. So if I would put that into a nutshell, I would say that while we invest billions of dollars every year in screening passengers and at the same time we leave the perimeter, I don't want to say unattended, but I would say unattended to a satisfactory level. What we actually do is invest all our resources on the front door and leaving the back door open. But at the end of the day it is the same aircraft that we are trying to protect by the screening that would be harmed by a relatively easy access of individuals through the perimeter.

So perimeter is certainly something that we have noticed in the past. It was discussed in this Committee, and I haven't seen a lot of development during the last few years despite the fact that it made a lot of headlines.

The other subject that made it out of headlines lately, is the issue of the threat of the insider, or in other terms when employees become part of an operation, to carry out illegal activity that could be also translated into terrorist threat immediately. We saw the case in Atlanta. Although here in this case I have to say that TSA had responded to it rather quickly by increasing the background checks and the frequency of those checks. But as we just heard from the other witnesses, there is still an open question about the quality of the background check itself, whether that really provides us with the security that we need.

And the third point that I'd like to refer to is the issue of how well do we protect the public and the employees at the airport against ground attacks as we witnessed a couple of years ago at LAX when an active shooter started shooting at the checkpoint and the security forces in the airport responded in a way that certainly can lead us to conclusions. There is a lot of room for improvement in this area.

The common denominator of all these three points that I made is that none of them are related to passengers, and yet they are falling back, even in comparison with the quality of screening pas-

sengers, and that means that the reason for that, in my view, is that in 2001, when TSA was established, it was established both as an implementer of security, as well as a regulator.

And I don't know any other example in government structures where an entity is actually regulating itself. There has to be a certain level of independence to the regulator, independence and authority, for the regulator to first of all, issue regulations that sometimes may not be comfortable for the implementer, but still have to be performed. And certainly when you look for the performance that doesn't meet the regulatory requirements but you are in charge of implementation, that's a conflict of interest, and I strongly recommend that the Committee will have a look at it and will consider a solution to that.

And the last point that I'd like to make is that, when we look at police forces in airports around the country, we see the more or less standard law enforcement organizations as we meet in the city center. But we have to understand that at the airport, the police function, the police priority should be security and prevention rather than law enforcement and reaction. Because when a terrorist attack takes place, it's all over. There's very little that you can do except deal with the damages. If we talk about explosive devices, and even when we talk about active shooters, they are willing to perform better. And that certainly calls for a different type of airport policing.

Airport police should be a dedicated, specialized force where the people are selected on the basis of their ability to perform those roles. They have to be trained and certified, and their certification has to be maintained. Exercises should be carried out on a regular basis, and at the end of the day, we have to make sure that the capability to prevent, or in cases where we need to respond, would be quick and effective. And this is not where we are today. Thank you very much.

Mr. MICA [presiding]. Thank you, Mr. Ron, and all of the witnesses.

[Prepared Statement of Mr. Ron follows:]

**STATEMENT BY RAFI RON**
**PRESIDENT OF NEW-AGE SECURITY SOLUTIONS INC.**
**TO THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM**

**May 13, 2015**

**Transportation Security: Are Our Airports Safe?**

Good morning, Mr. Chairman and members of the Committee. First, let me thank the Committee for inviting me to testify concerning airport security. I am Rafi Ron, President of New Age Security Solutions (NASS), a transportation security consulting firm based in Dulles, VA.

Prior to founding NASS, I served as Director of Security at Tel-Aviv Ben-Gurion International Airport for a period of five years. My experience includes more than 40 years in the field of security, intelligence, and counterterrorism. It is also my please to say that last year I became an American citizen.

Media reports in recent years have drawn attention to the security lapses that still exist in our airport security system. While much of the focus has been on passenger screening and security, passengers only represent a fraction of the risk we face. Little progress has been made securing the far larger portion of the airport where passengers do not have access. These challenges include:

1. Keeping intruders from breaching restricted areas of the airport, including parked aircrafts, the ramps and various locations of materials loaded later on aircrafts.
2. Protecting the public areas of terminals from potential bombers and "active shooters" and other types of ground attacks.
3. Preventing airport insiders from using their special access to restricted areas to help misguided individuals or terrorist cells, carry out illegal and destructive plans.

The common denominator in all of these challenges is that none of them relate directly to passengers. These risks are all within the "Airport facility security" domain, and outside the passenger and baggage screening protocols. This is not surprising in light of the fact that since 9/11 we have invested billions of dollars to screen passengers and bags but we have implemented very few and relatively inconsistent initiatives to improve ground security operations that would addresses the challenges reported by the media and other security lapses that are not publicly reported.

When setting a goal of protecting the aviation system, we cannot overlook the critical role of ensuring that each airport facility must stand as a security island, aware of risks in real-time, trained to respond quickly and equipped to thwart the higher levels of risk. Unfortunately, in our National Aviation Security strategy, intrusion prevention into restricted areas and other ground security vulnerabilities have become a lower priority. Consequently, we have seen relatively

uncontrolled access to parked or taxiing aircrafts. This has resulted in unauthorized vehicles on runways and taxiway as well as multiple examples of "stowaways" in the landing gear compartment of aircraft. One can only imagine the consequences if instead of 120 pound stowaway, an undetected intruder had left a two pound explosive device. Perimeter security is just as critical to aviation security as passenger and bag screening.

"The insider threat" to our aviation system is just as dangerous as the terrorist passenger but much more difficult to address because it comes from those who are already trusted inside the system. While inside criminal activity inside the US aviation system has not yet been directed at taking down airplanes, the perpetrators have demonstrated a willingness to defy the law and put others at risk. Although most aviation employees are honorable, hardworking Americans, recent reports indicate serious problems that range from firearm and drug to baggage thefts and inappropriate passenger contact. What is particularly troublesome is that the crimes are rarely the actions of an isolated individual. Networks of employees are flaunting the law and bypassing security for their personal motives. Such individuals are very susceptible to terrorist influences or inadvertently delivering explosive devises under pretext of "harmless substances" smuggling. As a result of the Atlanta weapon smuggling case, TSA is increasing background checks and the frequency for revalidating the clearances as well as random employee screening. These measures are important, but do not eradicate parallel breaches in the system.

Public area security is another vulnerability as we saw in the attack against TSA's agents at LAX in 2013 and the planned car bombs during the "Millennium Plot". Airports are not prepared for these scenarios despite the fact that they can be anticipated. Keep in mind that the same terrorists that have targeted the US aviation system, have repeatedly used car bombs, suicide bombers, and coordinated assaults against secure installations in other parts of the world.

An analysis of these diverse scenarios, demonstrates two main factors that contribute to our increased vulnerabilities:

a. There is no clear structure for responsibility, authority and accountability at most airports.
b. Even with the best of intentions, airport policing is not designed or implemented to meet the terrorist threats. They lack the officers, training, and equipment needed to anticipate and stop terrorist activities. For the most part, they are organized to deploy reactively rather than proactively.

The existing federal, state, and local structure presents two main problems:

TSA was established to take over passenger and bag screening. Previously the government regulated aviation security broadly through the Federal Aviation Administration. The FAA also provided grants and loans to help local jurisdictions enhance their facilities. Since screening was TSA's main responsibility, the federal government's role as a regulator for other aviation security activities was reduced in comparison. Even when TSA took on the Air Marshal program it was through executive implementation. So two of the main areas of aviation security became

federal self-regulating and issues like airport employee vetting, perimeter hardening, and local patrols became secondary.

This change in priorities led to the creation of a highly detailed screening operation, elevating the quality of screening substantially and consuming the largest part of the agency's budget. At the same time we see relatively little development in producing and enforcing new, higher standards in areas that are not the direct responsibility of TSA.

Perimeter security provides a good example of this problem. While passenger screening has increased, with comparably large budgets to support it, perimeter security standards did not changed much after 2001 and there is little federal budget support. The responsibility for executing perimeter security falls under the local airport authority. The lack of local government resources makes it difficult for TSA to issue and enforce higher standards to meet new challenges. TSA issues warning letters to airports with perimeter security breaches, but that has not proved to be very effective.

Good perimeter security is based on a combination of effective detection and surveillance technology, skilled manpower to assess alarms, and the ability to dispatch officers to prevent an intruder's access. At most airports, the technological systems are initiated and designed by an engineering department with little or no police involvement. The control center is operated by an airport operation department with limited security orientation. Patrols are typically provided by the airport police that in many cases operates under a system that places a higher priority on issuing traffic ticket. The result is that perimeter detection technology is not properly budgeted and designed, security control centers are not properly manned, and the airport police have limited presence on the perimeter even when alarm sound. No local, state or federal department feels responsible for the final result and in the absence of clear higher standards, we end up with very few airports actually installing and operating perimeter intrusion detection systems and running an effective perimeter protection.

This relates directly to the second major issue in the airport facility security operation. The traditional role of police departments is responsive. Legally and practically, this as the standard in law enforcement; the commission of a crime initiates action. When it comes to counter-terrorism, the goal is prevention because while a criminal rarely affects many people and wants to escape to have another chance, a terrorist doesn't. The paradigm is different because a terrorist wants to affect as many people as possible and is often willing to act without regard for their own life. By the time the event takes place, they have reached their objective. Response time is more a factor in treating the wounded than apprehending a perpetrator. Many airport police forces have not recognized the need to shift to a new mindset and strategy. Their mission, organizational structure, manpower profile, training, communications, and weapons in many cases have not changed after 9/11. This is not a negative reflection on them, as they are often simply preforming as they would in any other urban setting. But aviation security calls for different standards, with specialized training and a proactive orientation.

A good airport security system is based on systems that comprehensively prevent intrusion, instantaneously detect a breach and provide the ability to quickly reach any location on the airport. To be effective, it must function more like a security and protection team safeguarding a national security asset rather than traditional law enforcement patrols that may not need to visit a neighborhood for days. Airport police must be able to focus on the unique mission of an airport security force. Officers must be familiar with all the various possible terrorists Modus Operandi against their specific Airport. Manpower should be selected according to their ability to meet performance standards. And those standards should be created and guided by the reality that an airport is an integral part of our national security. Airport police officers should periodically be trained and certified at national centers that evaluate skills and fitness. They would benefit from exposure to national intelligence gathering and investigative capabilities focused on terrorist activities that jeopardize airport security.

Summary

In order to balance our aviation security system, we must reinforce the airport facility component. This can be achieved by having a clear and comprehensive regulatory environment that helps local airports prepare, train, and equip personnel as well as provide financial incentives to construct effective perimeter security systems. Prior to 9/11 that responsibility was within the FAA. After 2001, some of it was transferred to TSA. Some of it fell on the resources of local government. And some of it has been neglected. I urge Congress to take steps that would:

1. Create a clear structure of responsibility that extends from the national level to the "boots on the ground" level, including a predetermined local command structure for security emergencies. Identify airport police as the entity in charge of all aspects of facility security including planning, implementation, and regulation enforcement. And help them gain the tools to accomplish that goal by creation of a national training and certification program.
2. Create and enforce consistent standards for ground security measures, including perimeter detection systems that would balance the level of security with the programs implemented for screening and checking the background of aviation employees.
3. Select a federal entity that will develop standards for airport police forces nationwide that recognize their unique needs in the areas of mission statements, force building, organizational structure, strategy and tactics, weapon and other equipment, training, and intelligence.
4. Prioritize federal funding to enable resources to be allocated to local jurisdictions responsible for airport facility security.

Thank you for your attention, I will be happy to answer questions.

Mr. MICA. We're going to move now to a round of questioning, and I'll start. First of all, what you just said was interesting. You said TSA tries to do everything, and there are very few models of this. I think only Romania, Bulgaria, and some Third World countries have that structure.

And there should be some separation. The government should be in charge of security information, for example, getting the intelligence and preparing the list so even if you prepare a list, and you testified—well, first I'll let you respond. Am I correct in what I stated about the structure being flawed?

Mr. RON. Yes, you are correct.

Mr. MICA. So that's something again the Committee—we never set it up to have TSA continue to operate this huge screening force. Never in our wildest imagination would we imagine 46,000 screeners and 15,000 administrators. Stop and think about that. And, again, the report that has been released today, again you see why Carraway wouldn't show up. Just go over it. This isn't my findings.

Are you fairly independent, Mr. Roth? You're the inspector general?

Mr. ROTH. I am, sir.

Mr. MICA. Have you looked at this, and it's the whole truth and nothing but the truth? First thing, we conducted a series of covert penetration tests. I also asked the staff, many of the members are new. You have not participated in a closed briefing, you need to get a closed briefing and hear about the rate of failures. You will be appalled.

It's appalling, the failure rate—you don't have to give any specifics that are classified, but it's an appalling failure rate. Right, Mr. Roth?

Mr. ROTH. We are deeply concerned——

Mr. MICA. We have identified vulnerabilities caused by human and technology failures. We will set that up, in the Committee and Members of Congress. If audited TSA's acquisitions, point No. 2, the acquisition history is a complete fiasco. I cited the competing lobbyists and buying equipment that didn't work, people weren't trained for. And now the report back, OK, here's the GAO technology report, Ms. Grover, and you said in fact, you cited that some of the technology oversight in this report of March last year does not enforce compliance with operational directives. That's still the case, that TSA does not—in fact, I think from March 2011 through February 2013, about half the airports with AIT systems did not report any IED checkpoint results. Is this correct?

Ms. GROVER. Yes, sir, that's correct and——

Mr. MICA. And not much improvement according to what you found, Mr. Roth, on operation, training and auditing. Is that correct?

Mr. ROTH. That's correct.

Mr. MICA. OK. The third point. These aren't my points. This is what he found. We have examined the performance of TSA's work force which is largely a function of who is hired and how they are hired and trained and managed. Still problems with recruiting. Right, Mr. Roth? Still problems with training, Mr. Roth?

Mr. ROTH. Correct.

Mr. MICA. Still problems with managing. Right?

Mr. ROTH. Yes.

Mr. MICA. And their responsibility in conducting audit and oversight within the system. Right?

Mr. ROTH. Yes.

Mr. MICA. Audits have been repeatedly found of human error. And often a simple failure to follow protocol poses significant vulnerabilities. Is that your Statement, sir?

Mr. ROTH. It is, sir.

Mr. MICA. OK. Let's go to the last one here. We have looked at how TSA plans to buy, deploy and maintain its equipment. Well, I read the history, people don't realize that the threat is very serious and ongoing and that the bad guys are one step ahead of us. Just look at the history. The shoe bomber, TSA never detected it. Right?

Mr. ROTH. Correct.

Mr. MICA. The diaper bomber, never detected it. Right?

Mr. ROTH. Correct.

Mr. MICA. The New York Times Square bomber, he bought his ticket on the phone, went to JFK and went through all the screening systems and was not stopped until he got on the plane and it wasn't TSA. Right?

Mr. ROTH. That's my understanding.

Mr. MICA. OK. That's my understanding. But these are failures of this very expensive, $7 billion, 61,000 people, system. This is an indictment, and it's very concerning. The equipment failure is also very concerning because that's sort of your last line of defense. We have advanced imaging technology, and yet people are not trained to operate it or detect threats. Is that right, Mr. Roth? Is that what you found?

Mr. ROTH. We found significant human error.

Mr. MICA. And the last thing is, these guys are smart. When the members and staff get the next briefing, the thing that concerns me is right now all these systems are pretty much metal or nitrate based. Is that pretty much an assumption, that they detect metal or nitrates for explosives?

Mr. ROTH. I can't testify about that.

Mr. MICA. OK. Well, I can tell you that that is what they are. We tried to put in place a behavior detection system, which was a total failure. Other Committees have looked at how we did it. It's wrong. Israel does it, but Israel can profile. We can't profile. Israel can do other things that we can't do, and behavior detection as far as you're concerned and in one of these reports is a failure, too. That's looking at people, detecting behavior.

Mr. ROTH. Both the IG as well as GAO have done work on that.

Mr. MICA. And then finally, some of the safeguards aren't in place for the passengers' PreCheck system and making sure that we eliminate people who pose a risk. That's still the case? Yes or no?

Mr. ROTH. Yes.

Mr. MICA. That's still the case, Ms. Grover?

Ms. GROVER. Yes, sir.

Mr. MICA. And what's most astounding is this particular individual I cited before, the woman, was so notorious that the TSA officer identified her by other pictures he'd seen of the terrorist, went

to a supervisor, and she got not only a free pass, but expedited through TSA. That's a failure, is it not, Mr. Roth?

Mr. ROTH. Yes.

Mr. MICA. Ms. Grover?

Ms. GROVER. Well, the system in that case actually worked as TSA intended for it to work. That's my understanding.

Mr. MICA. But her data never came up because she was——

Ms. GROVER. She was not on the watch list.

Mr. MICA. Exactly. Exactly. So that's where we need to get this information, people who pose the risk we can identify, go after them or stop them.

Finally, the badge issue, the badge issue. Was it a couple of years that the TSA approved the badges at Atlanta where they gave badges out and didn't do the proper background checks. Is that right, Mr. Roth?

Mr. ROTH. We have done some work on that. In 2013, we had an audit where we found that the backlog was so great that TSA allowed airports simply to grant the SITA badges without a background check being done at the time.

Mr. MICA. And of the items that was cited by Mr. Ron, one of the issues is people inside the system who pose a risk; the perimeter also he mentioned, which poses a risk that we don't have systems in place for; and then the outdated structure that we have where TSA tries to do everything and does nothing very well, which is well-documented by your report.

Thank you, Mr. Roth. And I yield now to Ms. Maloney, the gentlelady from New York.

Mrs. MALONEY. I thank the panelists for your testimony and your work, and I thank the ranking member and chair for calling this important hearing. And I agree completely with the Statements of Mr. Roth when he said that the terrorist only has to be right once. We have to be right 100 percent of the time. We have got to stop them from coming through.

I would say nothing is more important than protecting our people. And I will say that since 9/11, the New York City Police Department has documented well over 17 attempts to murder New Yorkers, and they have been thwarted through the combined efforts of all of law enforcement, including TSA, which is working every day to stop it.

For some reason in our classified intelligence briefings, airlines continue to be a top priority for terrorists, a top target. They keep trying different ways. We hear it from press reports, your reports, and reports from airline stewardesses and captains of how they're trying to break the perimeter, how they are trying to get into the cockpit in different ways. And so I see this as a collective effort to fight back. It's not just TSA but all of us working with them to fight back.

The PreCheck program, we also need commerce to work, and at first airlines were so backed up people weren't even flying anymore. I will say now that in New York the PreCheck program is a success. Now the PreCheck line is longer than the normal line. More people are in the PreCheck line than in the other, so many people are in it, which I think speaks well that we have processed a lot of people and made it more efficient.

So I want to ask Ms. Grover, apparently 33 percent of the passengers now pass through PreCheck. Is that correct? About how many people are in PreCheck now, would you say?

Ms. GROVER. Well, the last data that I saw was almost half were receiving expedited screening in one form or another.

Mrs. MALONEY. Half were receiving it in one form or another.

Ms. GROVER. Right.

Mrs. MALONEY. That is a remarkable achievement from where you started. I see this also an effort in many ways we are trying to crack down also on terrorist financing. Many of the banks are complaining about having to do PreCheck or they have to validate every single one of their customers, and there's been some ideas about letting their system work with Homeland Security on combining a PreCheck list. They have to report, you have to report, on who's in PreCheck. I think that's a valuable new tool that we could look at in making it more efficient and also stopping more people. And I wonder, Ms. Grover, what you think about that, and I have a proposed outline of a pilot project in that area that I'd like you to look at and have your department get back to us.

Ms. GROVER. Thank you. We would be happy to do that. Right now the background check for individuals who sign up for PreCheck are conducted by TSA, and it includes a criminal background check, a check on immigration status, and a third aspect of the check, and that's against the terrorist screening data base. And so I'd be interested in talking with your staff about the specific work you'd like to do in terms of opportunities to expand that.

Mrs. MALONEY. Well, there are other units in our country that are also doing background checks, so if we could compile them together and make it more efficient and knowing who these people are and increasing our ability to keep the bad people out of New York or out of the country, out of the country period. But as one who represented many people, many families who perished on 9/11, it's an issue of grave concern to me. And when we created this whole system of review at airports, it was hotly debated whether it should be private or government, and many believed that our police and fire, who are charged in protecting us, are government. And TSA has the same level of importance in protecting our people and are now a huge target area which continues for some reason, airlines. I believe it should remain a government function. It's too important, protecting lives of citizens. There is a movement in Congress to privatize it. I'm opposed to that. I believe it would weaken the system, not strengthen it.

But I welcome this hearing of ideas of how we can strengthen this very important program. But the bottom line, we haven't had another tragedy in a long time. When was the last time we had—we had many attempts—but when was the last time there was a terrorist attack that was successful on the airlines? Ms. Grover.

Ms. GROVER. Well, I guess the 2009 attack would probably be the last significant one.

Mrs. MALONEY. And what happened in 2009?

Ms. GROVER. And that was an attempt to take down an airline. It was the gentleman that was bringing explosives on to the plane, and that was stopped on the plane. And in response to that, TSA put additional systems in place to be able to detect nonmetallic ex-

plosives, and they also started expanding the watch lists. But as part of our work we have found that there are weaknesses in the ability of the current systems to be able to identify even all of the people who are on the watch list. In fact, there are still errors in that. We also have work that has exposed weaknesses in the AIT systems and TSA's knowledge of how well they work; so there is still work to be done.

Mrs. MALONEY. Well, it's a work in progress, and the bottom line, it was stopped. And so we join you in your efforts, and thank you for your testimony. My time is expired. Thank you.

Mr. MICA. Thank you. Mr. Walberg.

Mr. WALBERG. Thank you, Mr. Chairman. Mr. Ron, why do you believe preventing perimeter breaches should be a top priority?

Mr. RON. Sir, would you repeat the question?

Mr. WALBERG. In your testimony you mentioned perimeter breaches. You mentioned a wheel well situation, but why do you believe perimeter breaches should be a top priority?

Mr. RON. Because at the end of the day, everything that we do at the checkpoint can be boiled down to the need to prevent a passenger from bringing an explosive device or a weapon that will allow an attack against the aircraft, the flying aircraft. The same target can be achieved simply by breaching the perimeter. The problem with breaching the perimeter is that—we have reports about 230-something cases that the Associated Press reported lately, but those are the cases that we know about.

Keep in mind that most airports around the country do not have a detection system on their perimeter, and therefore one could enter and leave the airport without leaving any traces. There's no systematic way to prevent that. And if at the end of the day that leads to the same result that we are trying to prevent at the checkpoint, I would consider it as being critical.

Mr. WALBERG. Kind of negates all the effort then. Do you think that TSA is taking theinsider-outsider threat seriously?

Mr. RON. I think that the fact that there's a division between Federal responsibility and local responsibility. It leads to the failure to upgrade standards on perimeter security. While when it comes to a direct responsibility and implementation responsibility of TSA, we see all the resources available, and the screening operation takes the major, almost all of TSA's operational budget. When it comes to perimeter security, it is expected that the airport will take care of that. The airport doesn't have neither the manpower to do that. The number of police officers is too short for that.

The ability to invest in a detection technology around the perimeter, which doesn't come cheap, is also very limited. If in the past, and I have referred to prior to 9/11 when FAA was the regulator, only the regulator, and it also controlled the AIP program which provides grants to airports for improvements, security was part of it. Now the security is not very much a priority for FAA because it has pushed toward a DHS court. The idea of funding those, the necessary steps, is falling between the chairs.

Mr. WALBERG. So the coordination is out of whack as well with the resources. Let me just move on. I'm asking each of you to respond to this question. Do you believe TSA overprescribes technological solutions and fails to think creatively about airport security?

Mr. RON. Yes, I do. I think that basically we do not pay enough attention to the passenger himself. The fact that we have started implementing steps in that direction, like PreCheck, should be welcome, although we need to carefully look carefully at what is being done as was suggested here earlier. But I think it is a step in the right direction. I also think that behavior detection is a part after it, but obviously I have a dispute on that with some of the other witnesses here.

Mr. WALBERG. Ms. Grover, could you respond?

Ms. GROVER. I would answer your question by saying that I think TSA is overemphasizing getting the programs up and running and underemphasizing evaluating their effectiveness, regardless of whether we're talking about technology solutions or other solutions.

Mr. WALBERG. Are we looking imagination and creativity?

Ms. GROVER. You know, TSA is open to different options, and they put different strategies in place; but creativity is not helpful if TSA doesn't have evidence to show it works.

Mr. WALBERG. Mr. Roth.

Mr. ROTH. Just briefly, yes. I believe that the best technology solutions in the world, if the work force is not trained to use them, does not follow the protocols that they're supposed to use, is useless.

Mr. WALBERG. I guess my concern is as I've traveled through Detroit and Washington most generally, I see TSA agents attempting to perform their functions in most cases with courtesy, doing their jobs as it's clear they have been told to do. But I just wonder if there aren't some great ideas that could come from TSA agents themselves that people like Mr. Carraway and others aren't willing to listen to or aren't given time to listen to, on how to deal with our passengers and our security risk, which includes the perimeter. Because they hear about it just like us and know for a fact that all that they've done at the PreCheck line or the general line can be taken out of any type of positive results simply because we haven't looked at all the places we could go.

So thank you for your testimony. I see my time is expired. I yield back.

Mr. MICA. Mr. Lynch, you're recognized.

Mr. LYNCH. Thank you, Mr. Chairman. Mr. Chairman, if I could just ask, I know that because of the scope and depth of the problem here, Mr. Carraway's attendance here would be very, very important. I'm just wondering if the Committee has any plans to subpoena him, Mr. Chairman?

Mr. MICA. I honestly don't know. I discussed that with the staff before——

Mr. LYNCH. Can I yield to the ranking member?

Mr. CUMMINGS. What was the question?

Mr. LYNCH. Well, the fact that—I mean, we got some wide problems here, from perimeter security to people that are on the PreCheck list that are felons, and it's a pretty wide gap in our security. And Mr. Carraway's attendance would be extremely important to us, and I'm just wondering, are we going to get him in here because a lot of my questions are for him?

Mr. MICA. Same here. Oh, you yielded.

Mr. LYNCH. I did want to ask the ranking member.

Mr. CUMMINGS. Chairman Chaffetz and I did discuss this. He was trying to avoid a subpoena. What we were going to try to work out—and I mentioned it a little bit earlier in my opening—I agree, we really do need Carraway here, and so I asked the chairman to set a date certain for him to come in so that we can get him in here to ask questions, because you're absolutely right.

Mr. MICA. I would agree with Mr. Lynch, if you would, you asked me in the beginning. We talked about it with the chairman, and I would be supportive of a subpoena if necessary.

Mr. LYNCH. If it's needed, I just want to voice my support for that as well. And the fact that the gentleman is not here sort of feeds into the whole narrative here that we have a bureaucracy that's not really responding to the problem that's out there. But I do want to thank the witnesses who are here. That should not diminish your attendance. I appreciate your valuable testimony. It's already been helpful.

As I said, we have got some major gaps in security. There have been several notable security breaches. I note that on September 14, 2013, a TSA employee was arrested along with five others for participating in a scheme to smuggle undocumented immigrants into the United States.

Additionally, two airline employees were arrested in December 2014 for smuggling weapons, guns and ammunition, on at least 20 flights from Atlanta to New York over an 8-month period. And two TSA security screeners at San Francisco International Airport were also arrested in March 2015 for allegedly operating a drug-smuggling conspiracy. In addition, on March 9 there was a report that was in the press. I believe NBC had a story about these 1,400 badges that were—and these were security badges for employees to access secure areas. They had gone missing over roughly 2 years. That was at the Hartsfield-Jackson Atlanta International Airport.

And as well, in the city of Boston, there's closing arguments today on the death penalty question for one of the Marathon bombers; and the brother who is now deceased, was missed. He actually left the United States, left Boston. Went to Dagestan. We had a report from the Russians to our security offices, the FBI and the CIA, to alert them that he had been engaged in alarming behavior, contacting terrorist groups in Chechnya or Dagestan. And he was on the TIDE list, 700,000 names.

So this is widespread. Mr. Roth, you've done a great job in terms of authenticating some of the gaps here, but do we need to give you more power to actually try to address some of this stuff? There seems to be a division of labor here between the airports and the TSA in terms of whose responsibility it is to set these security protocols?

Mr. ROTH. It is a massive job. When you talk about the number of SITA badges that are out there. For example, in 2012, we reported that there were 3.7 million badges for secured areas, so the idea of trying to keep that secure with that size, 450 airports across the country, it's just a massive job; 50,000 TSOs, 46,000 transportation security officers. We have initiated a number of criminal investigations against individuals, which is I think typical

any time you get a work force that size who has that responsibility, so it is a massive job.

Mr. LYNCH. Is there a lot of turnover among these TSOs, transportation security officers?

Mr. ROTH. I have not looked at that. I'm not sure if GAO has looked at that or not, but I'm not sure.

Mr. LYNCH. Well, I actually think a lot of the things we need to talk about probably are going to have to take place in a classified briefing unfortunately, so I won't waste any more time. So I look forward to that opportunity. Thank you. I yield back.

Mr. MICA. Mr. Grothman.

Mr. GROTHMAN. Thank you. I have just have a couple questions. First of all, you said before, how many supervisors do you have as part of TSA?

Ms. GROVER. So I'm not sure exactly how many supervisors there are, sir. That would be a better question for TSA.

Mr. GROTHMAN. OK. None of you up there would even have an opinion?

Mr. ROTH. We have not looked at that policy.

Mr. GROTHMAN. OK. When you review or when you audit them, I have heard from TSA agents that they feel that there's some overstaffing going on here. Do you concur with that, or do you feel there is? Or do you think they're trying to do what they can to kind of tighten things up a little?

Ms. GROVER. So we haven't looked specifically at the question of whether or not there is too much in the supervisory area. But we did do a report in 2013 that looked specifically at the issue of misconduct and found that there were about 9,600 misconduct cases that were adjudicated by TSA over a 3-year period, and at that point the total personnel was about 56,000.

Mr. GROTHMAN. How many?

Ms. GROVER. Total personnel was about 56,000 I believe at that point, and so I would say there is certainly a need for some supervision.

Mr. GROTHMAN. OK. Could you give me, rattle off like the three major causes of doing things wrong, and misconduct?

Ms. GROVER. Sure. The largest category of misconduct was attendance and leave issues, so essentially being absent from work without prior approval or extensive tardiness. The second category of misconduct was screening and security errors. That counted for a full fifth, 20 percent of those roughly 10,000 misconduct cases; and those would be instances where the SOPs were not followed, such as screeners allowing individuals or their bags to bypass screening or where TSOs were bypassing the equipment check, so those are types of misconduct cases that could lead to a degradation of security.

Mr. GROTHMAN. So collectively you feel, if anything, they ought to be tightening things up a little bit more?

Ms. GROVER. I don't know if that necessarily translates to a need for additional supervisors.

Mr. GROTHMAN. Oh, no, no.

Ms. GROVER. But certainly, yes, there is room for addressing those issues.

Mr. GROTHMAN. OK. Well, different people have opinions on that, but thanks. I will yield the rest of my time.

Mr. MICA. Thank you. Just on your time. Now, the figures we have are that there were 61,000 TSA personnel, that's the latest that I had. And we had a cap of 46,000 screeners, so which leaves you with about 15,000 people who are not screeners; is that correct? And we had just under 4,000 people in Washington, DC. within the close proximity making on average $104,000 apiece, pretty hefty overhead, wouldn't you say?

Ms. GROVER. Thank you, sir. I am not familiar with the exact numbers. Those sound right to me.

Mr. MICA. Those are pretty close. But we've built a huge bureaucracy, never intended it to be that way, and we've got to get it under control, better managed, whether it's training, acquisition of equipment, performance, the passenger facilitation systems that don't work, a lot of deficits.

And then Mr. Ron mentioned the issues of perimeter security, I just visited an airport this past week in Knoxville, and looking at their vulnerabilities, but you can take any airport and just, whether it is LaGuardia where you can get a little rubber raft and end up on the runway, or any major airport in the country is easily penetrable by their perimeters, some of the issues you raised, Mr. Ron.

Let me conclude—I yield back your time. You have the——

Mr. GROTHMAN. Just one question.

Mr. MICA. You have the time.

Mr. GROTHMAN. A few years ago they instituted these new things to see through you or whatever, they were kind of controversial at the time. Have you ever thought about restricting their use or could you just comment in general on them?

Mr. ROTH. What you're referring to are what's called the AIT machines, which is Advanced Imaging Technology machines, where you have to sort of put your hands up and then the things go. We are doing some covert testing on that as we speak. We'll write a classified report with regard to that. Early returns give us some concern.

Mr. GROTHMAN. Concern of what nature?

Mr. ROTH. Whether they are effective.

Mr. GROTHMAN. Good, maybe you won't need them.

Mr. MICA. Well, I might point out just for the record that—and I pointed it out at the beginning, I don't know if you were here, sir, but the acquisition of that equipment was very controversial, and Mr. Chaffetz objected to them buying some of the equipment that was—what he felt violated people's rights. They went ahead and split the contract, as I mentioned, between Mr. Chertoff's client, which was Rapiscan, and then between L3, which was Nastachel, a half billion dollars worth of contracts split evenly. They ended up the Rapiscan could not be changed so that it wouldn't violate people's privacy and those—that equipment after being installed was pulled out.

So we've been through that three-ring circus, now that this report focuses on the deployment of some of that equipment, for example the advanced imaging detection which is millimeter wave, where you put your hands up. And we have problems with main-

taining the equipment, operating the equipment, auditing the performance of the equipment all outlined by these witnesses.

Mr. DeSaulnier, the gentleman from California is recognized.

Mr. DESAULNIER. Thank you, Mr. Chairman. Let me begin by opening comments recognizing the enormity of the responsibilities that you have and assuming there have been many successes. But Mr. Roth, I wanted to talk about really two subject areas, and Mr. Ron, the second part is the perimeter given that I'm from the Bay Area and we've had a lot of news coverage on that case and other cases.

But Mr. Roth, you mentioned in your opening comments that complacency is a huge problem and that human error is too common and basically it's—the human error is simply to follow protocol. And also you mentioned that you have to be—TSA has to be right every time and a terrorist only has to be right one time. So we have lots of examples in proper quality assurance in different fields, in similar situations, at hospitals or industrial facilities. Is there a basic—or maybe Mr. Ron knows this or Ms. Grover, a basic management tool when you have these kind of situations to make sure that complacency isn't the order of the day?

Mr. ROTH. I think it is severalfold. You know, one is oversight, TSA itself has what they call I think red teams, which go in and do testing on systems and individuals to ensure that they get it right. We obviously do covert testing as well. And then I think it is it is a matter of training. As in the military, if there is a training culture that you do a certain protocol the same way every single time, then you're going to at least lower the incidence of human error.

Mr. DESAULNIER. So that's not sufficient in this instance, is that your view?

Mr. ROTH. The results that we have found have shown that there is room for improvement.

Mr. DESAULNIER. Is there in your view misprioritization? Should there be more emphasis on this as opposed to technology?

Mr. ROTH. I think there needs to be more of an emphasis on training, yes.

Mr. DESAULNIER. Mr. Ron, your comment about very alarming that we put a lot of emphasis on the front door, but the back door is wide open, and given your comments and your experience both in Israel and Massachusetts, are there best practices both on a low-threshold cost, sort of a medium and higher level? Because you also mention basically we don't have the resources to do the higher level.

Mr. RON. Thank you. I think that one thing that I find missing at the base is the lack of comprehensive approach to the challenges of aviation security. We are defining the relatively narrow angles and we take care of those angles, but sometimes we miss the wider picture.

I think again that perimeter security is a perfect example for that, because while we're trying to prevent exactly the same event on one side of the operation we invest a lot and on the other side of the operation we allow the situation to remain as poor as it is for many years, despite all the red lamps that they blink at us.

Mr. DESAULNIER. So in your previous experience you had to balance your resources, your funding with the risk assessment. Are we doing that sufficiently in this instance?

Mr. RON. Yes, I think that risk assessment is an ongoing process. It has to be part of our operation continuously. It needs to be present all the time. It has to be done at every level. So when we talk about passengers, for example, there's room for individual risk assessment per passenger in order to identify the of level of risk of that passenger. I think that the criminal background check is not enough. For that——

Mr. DESAULNIER. I was speaking more about in relationship to the front door to the back door. Are we putting enough? Is this a proper risk assessment that we should put more in the front door and not on the back door? You implied in your opening comment that we weren't.

Mr. RON. Yes, my answer is reasonable for that as well, yes.

Mr. DESAULNIER. Ms. Grover, do you care to comment on either the complacency problems or the perimeter problems?

Ms. GROVER. Yes, sir. In earlier work that we did looking at perimeter security issues, what we found is that TSA had not been able to do a complete risk assessment because they weren't sufficiently assessing the vulnerability of different airports. They have since made steps in that area and we do have a review underway now to look at that issue.

The other thing, the other issue that I would raise to TSA is a question about whether or not they are making adequate use of the data that they have. They do require airports to report all incidents to TSA, but when we looked at that data set previously we found that it wasn't organized or reported in a way that TSA could specifically identify how many of those incidents were related to perimeter or access breaches. Again, they have made some changes and so we'll be able to report back in the future on whether they are able to analyze that data.

Mr. DESAULNIER. Thank you. Thank you, Mr. Chairman.

Mr. MICA. I thank the gentleman. Mr. Hice is recognized.

Mr. HICE. Thank you, Mr. Chairman. This past February NBC News reported that over 1,400 security badges were missing in Hartsfield-Jackson Atlanta International Airport just over the last 2 years alone. Mr. Roth, could you briefly explain how TSA responds when some of these security badges turn up missing?

Mr. ROTH. We are doing some ongoing review of TSA's security controls, so my answer will be preliminary, but my understanding based on my conversations with TSA officials is once a badge goes missing, it is turned off. So this has to be sort of a two-factor authentication, you have to take the badge and swipe it to be able to enter secure areas.

The difficulty of course is this idea of piggybacking, somebody else opens the door and you walk through, or other ways to be able to gain access to these secure areas. And that is the whole challenge behind these access badges, right? If you work in a McDonald's at the airport, you get a badge, and then you quit the next day and you still have that badge. And it's incumbent on the airport to report that to TSA so that badge gets turned off, and it is a vulnerability.

Mr. HICE. So you would say that the responsibility rests then with the airport, not with TSA?

Mr. ROTH. It is a joint responsibility, as I understand it.

Mr. HICE. Right, it ought to be a joint responsibility. And the airport—Atlanta airport was just the only airport reporting on that particular study, 1,400 badges missing in 2 years. How many would there be across the entire Nation?

Mr. Ron, just a yes or no type question regarding this, would you consider 1,400 just out of one airport security badges showing up missing a major security breach and a potential problem?

Mr. RON. Well, obviously it is a matter of proportions. Atlanta is one of the largest airports in the country and I assume that the number of badges that they issue is larger than most airports around the country, and I do not know what is the percentage, but I would say that every airport the worldwide that I know suffers from that problem.

Mr. HICE. OK, my question, is this a security threat of significance that needs to be looked into, yes or no?

Mr. RON. It is, it is.

Mr. HICE. OK, all right. That's—because obviously we've got a major problem here. We've got badges that are missing, stolen for whatever reason, but to the tune of thousands across the country. And what I'm hearing from you, Mr. Roth, is there's really no—at least to your awareness—no policy to deal with this. And yet we've got a major potential security breach going on here of insider threats, really.

Assess the, real quickly, the vulnerability of insider threat?

Mr. ROTH. Well, if you have access to secure areas, that means you have access to the aircraft, the dangers there I think are self-evident.

Mr. HICE. All right. Let me go back to another situation in Atlanta, Mr. Roth, and I'll just continue with you. As we all know, there was a gun smuggling insider ring at the Atlanta airport that was discovered this last December. To your knowledge, has there been any changes in security checks and so forth since that gun smuggling ring was discovered?

Mr. ROTH. As I said, we're in the middle of an audit of this exact problem, so unfortunately I can't give you a complete answer as I sit here today.

Mr. HICE. Should there be changes?

Mr. ROTH. Oh, absolutely.

Mr. HICE. All right. What changes would you suggest?

Mr. ROTH. Well, at this point I think I'd have to defer until we get our audit completed so we can make recommendations to TSA, first figure out what it is that we find and then make recommendations that make some sense.

Mr. HICE. All right. What kind of—what needs to be done with verifying that those who have security badges do not have a criminal history?

Mr. ROTH. We are about to come out with a report with regard to that, to check the TSA's efficacy on doing criminal background checks. And I know GAO has done some work on that in the past.

Mr. HICE. How many background checks are there?

Mr. ROTH. Well, there would be one for every TSA employee who has a SIDA badge. So——

Mr. HICE. OK. So in that scenario, there would be one background check. Is there anything to protect the public from one of these individuals getting involved in criminal activity after they have already had the initial check?

Mr. ROTH. No. And you know, we have a number of investigations that are set forth in my testimony in regard——

Mr. HICE. Should there be?

Mr. ROTH. Well, absolutely there needs to be vigilance or criminal investigative presence against the TSA employees.

Mr. HICE. I would ask you please to report back to our office on this type of thing. I would very much appreciate it.

Mr. ROTH. Absolutely.

Mr. HICE. Thank you.

Mr. MICA. Thank the gentleman.

Mr. CLAY.

Mr. CLAY. Thank you, Mr. Chairman, thank you, Ranking Member Cummings for conducting this hearing. I appreciate the efforts to streamline the security screening process for low-risk individuals and shift focus to those who are deemed at higher risk. My understanding is that all airline passengers are compared to Federal Government terrorism watch lists through the Secret Flight program. Ms. Grover, is that correct?

Ms. GROVER. Yes, sir, that's correct.

Mr. CLAY. OK. But only individuals enrolled in the PreCheck Program are also checked against other law enforcement lists such as immigration and criminal data bases; is that correct?

Ms. GROVER. If they apply for PreCheck, then yes, then they are checked against the criminal background information.

Mr. CLAY. And the PreCheck program requires individuals to self-report any new criminal activity or convictions after they are enrolled. In other words, individuals have to self-report any new crimes; is that correct?

Ms. GROVER. Sir, I'm not actually sure if that's true for PreCheck. I do know that's the case for the aviation workers at the airport, that there is no followup background check, and I believe the same thing applies to PreCheck as well.

Mr. CLAY. Mr. Roth, does this self-reporting requirement pose a potential security risk?

Mr. ROTH. It does. And in fact, in the PreCheck program it does require self-reporting, there is no continuous pinging of the criminal justice system to figure out whether, you know, if I apply for PreCheck and then I get convicted of a crime a year later my PreCheck is still good for 5 years. If I don't report that to TSA, TSA is not going to know about it.

Mr. CLAY. Any idea of how many have self reported?

Mr. ROTH. I don't have that information.

Mr. CLAY. Ms. Grover, any idea?

Ms. GROVER. No, sir.

Mr. CLAY. OK. Ms. Grover, GAO's recent report identified instances in which Secure Flight did not accurately identify passengers on government watch lists; is that correct?

Ms. GROVER. Yes, sir, that's right.

Mr. CLAY. What were GAO's findings with regards to the ability of Secure Flight data appropriately designating individuals at low risk?

Ms. GROVER. So the Secure Flight system, the first thing that it does is it's used to identify individuals who are on the watch list. And we know that sometimes that there are errors there, that Secure Flight doesn't always identify people on those high-risk watch lists. So after that set of identifications is done and those people are tagged, then the remaining passengers are also screened to see if they are a known low-risk traveler, and that's the way that they are then identified for PreCheck.

And then there's another tier where there's some automated assessments done where people can get additional PreCheck, that's how come sometimes PreCheck shows up on your boarding pass even if you haven't signed up for it in advance.

Mr. CLAY. What measures can be taken to ensure that Secure Flight accurately assesses the risk level of all passengers?

Ms. GROVER. We've recommended that TSA should have a new performance measure in place so that they can keep track on an ongoing basis of how well Secure Flight is doing actually identifying everyone on those Federal watch lists. And they are working on it, but that is not in place yet.

Mr. CLAY. Then how do you keep from I guess stereotyping or profiling travelers? I mean, what are the precautions put in place to not do the profiling?

Ms. GROVER. Well, that issue would be most relevant, say, at the airport when individuals are being selected, say for Managed Inclusion. And the TSOs are supposed to use like iPads that have randomizers in there, so there should be some protection from profiling there. But there have been questions raised about the behavior detection officers over many years about whether profiling could be factoring into their decisions, and they are part of that Managed Inclusion process.

Mr. CLAY. OK. Mr. Roth, you made 17 recommendations to TSA in your March report, and many of them dealing with the ability of the PreCheck initiative to effectively assess risk level of the individual. Can you briefly walk through the areas you see as needing improvement?

Mr. ROTH. Unfortunately most of those are either sensitive security information or classified, so it is difficult to talk about them. But we have made recommendations that TSA really needs to rethink how it is that they use the risk assessment rules. They have largely disagreed with our recommendations.

Mr. CLAY. That's unfortunate. Thank you all for your responses. And Mr. Chairman, I yield back.

Mr. MICA. You have 9 seconds, if I could have them.

Mr. CLAY. Sure, I yield.

Mr. MICA. Just a couple of points. You testified that the employees—well, first of all, they are not checking the backgrounds before they are employed, that's part of your finding—and the worst instance was Atlanta. Then they are not checking afterwards. In other words, there is not a check if they appear on some criminal list or watch list afterwards that's correct on employees.

And then I wanted to know about PreCheck. Is there any going back and checking people after they've been cleared for PreCheck? I know in Israel they control whoever gets sorted to PreCheck, and then they are always reexamining those individuals and the information is brought in, and they can stop the pass or access from the information that is concurrently and continuously being examined. Tell us about PreCheck and employees.

Mr. ROTH. My answer, Mr. Clay, was referring to the PreCheck employees, that there was no recurrent vetting and it required sort of a voluntary disclosure. I'm not sure about the employees.

Mr. MICA. Do you know?

Ms. GROVER. So with respect to PreCheck enrollees, the only recurrent check is that they would be checked against the Federal watch list every time, but not for criminal background. And as far as aviation workers, it's basically the same thing. They are checked regularly against the Federal watch lists. Although TSA has recently announced that they are going to start redoing criminal background checks every 2 years. I don't know if that's in place yet.

Mr. MICA. OK. Thank you. Mr. Duncan.

Mr. DUNCAN. Well, thank you, Mr. Chairman. And I apologize to the panel because I've been at another hearing and I'm trying also to meet with constituents, but I did want to ask about something in Mr. Ron's testimony that really stood out to me. You say although most aviation employees are honorable, hardworking Americans, recent reports indicate serious problems that range from firearms and so forth and so on. And so what is particularly troublesome is that the crimes are rarely the actions of an isolated individual, and networks of employees are flaunting the law and bypassing security for their personal motives. Such individuals are very susceptible to terrorist influences and so forth.

Now, I know that a lot of times with this 24-hour news cycle, we're almost sensationalizing even minor incidents. But that seems to me to be a pretty sensational type Statement, Mr. Ron, when you say networks of employees. And I'm wondering, I know you mention the Atlanta incident or the Atlanta smuggling, but I'm wondering, is this oversensationalized or is this happening in all the major airports? You say networks of employees. How widespread is this?

Mr. RON. Most of the crimes that could generate benefits for employees that are willing to act criminally are involved with illegal materials like drugs and weapons that fly through the airport. It is never a single individual person that is involved. Usually there is somebody who delivers the substance. There is somebody who actually takes care of it and puts it on the aircraft.

And if I take for example a case, of a few years ago, concerning a flight from Miami to San Juan, Puerto Rico. Once again, there was a matter of weapon smuggling through the aircraft. It was a duffle bag, if I'm not mistaken, 14 different weapons, including an AR–15——

Mr. DUNCAN. But you said that's a case from several years ago.

Mr. RON. That's several years ago, yes. But this indicated—this case, that was brought by one employee into the restricted area. There was another employee that actually took the flight and received the bag in order to fly with the bag to San Juan according

to media reports. So this is I think a very good example as to how these things work. You can assume that similar involvement of more than one person is the case more frequently than otherwise.

Mr. DUNCAN. Well, let me ask you something else, you were director of security at the Tel Aviv airport, I understand. What are some things you were able to do in Tel Aviv that people in your similar security field wouldn't be able to do or aren't doing here?

Mr. RON. Well, Tel Aviv system is based very much on our ability to recognize the level of threat of individual employees, based on a much deeper background check to start with. And they are implementing——

Mr. DUNCAN. So we need to give much deeper background checks to all airport employees?

Mr. RON. Well, there is a lot of—yes, background checks is one very important rule.

Mr. DUNCAN. All right.

Mr. RON. Beyond that I would say—and that has to do with the smaller size of Ben Gurion Airport in comparison to airports like Atlanta. But we were able to actually keep our finger on the pulse in terms of what happens with the employees at the airport. If somebody was behaving in a way that indicated that he may be involved in illegal activity, then we were immediately investigating it. There was a dedicated—there is a dedicated unit that is actually looking exactly only after that. They are making sure not only concerning security but also concerning regular criminal activity——

Mr. DUNCAN. So do you think we should have some type of incentive programs for airline—airport employees that turn in or recognize unusual criminal activity or something?

Mr. RON. I'm sorry, I didn't understand the question.

Mr. DUNCAN. Well, in other words, should we teach other airline employees or airport employees things to watch for when you say that airport employees are acting in unusual ways?

Mr. RON. Yes. I mean, obviously, there is—at the end of the day there is limited access to every badge holder, but when you speak about employees, this is different because by the way badges are also issued to non employees. But in the case of employees, we are able through the human resources and through our intelligence activity at the airport and through our ability to survey a city, those parts of the airport that are vulnerable to criminal activity in a way that makes it very effective.

Mr. DUNCAN. Let me ask, I've run out of time. Let me ask Mr. Roth one last question. Mr. Roth, we're spending mega billions now for security at the airports when you add it all together. Are we getting a bang for our bucks? Or——

Mr. ROTH. I think there is significant room for improvement. It is a massive task. I mean when you talk about, for example, security background checks on individuals that hold the passes to the secure areas, you're talking about 3.7 million people that you would have to give a background check for. This is a massive, massive challenge.

Can TSA tighten up? Absolutely. And the reports that we have written over the course of the years I think show there are areas where they can tighten up, but we need to understand the scope and significance of the problem that TSA faces.

Mr. DUNCAN. All right, thank you very much.

Mr. MICA. I thank the gentleman. If FedEx can track a package and American Express can detect instantaneously from an incidence with your credit card, certainly we can get this right and have many more people to deal with. Let's yield to Ms. Kelly from Illinois.

Ms. KELLY. Thank you, Mr. Chair, and thank you, Ranking Member Cummings, for holding a hearing on a pressing issue like our aviation security. I would also like to thank our witnesses who have taken time out of their busy schedules to speak with us today.

Mr. Chairman, with the summer travel season fast approaching, our Nation's airports will be pressed to the maximum capacity. This means long security lines, overworked TSA agents and control tower officials. It also means detecting and neutralizing a security threat in a crowded airport can be as difficult as finding a needle in a haystack. This is something all Americans, and of course my constituents in particular, know all too well. The greater Chicago area is currently served by two airports. I'm sure most people in this room here today at some point or another have missed a connecting flight or had a long layover in one of our airports. I hear complaints from my colleagues all the time. A culture of delays, overcrowded hallways and long security lines are not only frustrating and inefficient, but also unsafe. A need for a third airport in Chicago has been known for years.

I have been working with Secretary Foxx and Administrator Huerta to make a south suburban airport a reality. I am pleased to say that the project is close to becoming a reality and I will continue to push for its creation. Therefore, I'd like to ask the witnesses to provide their insights into this matter.

How does the fact that major airports are operating at capacity impact our national security? I'll ask both my questions. Impact our national security. And the other, would construction of new airports improve our national security by easing pressures on current airports? And whoever wants to take the question.

Ms. GROVER. So I can start. I agree with the other panelists that TSA is pressed, just the press of business is difficult. And as airports are operating more and more at capacity, there are some inherent challenges that go along with that. But what I would suggest is that the challenges that TSA faces in improving security across their systems are independent of exactly how many airports we have up and running and exactly whether they are working to capacity, because they are inherent systemwide efforts, and I'd like TSA to spend some more time focusing on how well their systems are working.

Mr. RON. I want to repeat a point that I mentioned earlier that I think is relevant to your question, and that is once again the need to approach the subject or the challenge comprehensively. Right now, in my view, this is one of the weakest points in the strategy, because of a lack of comprehensiveness, we do leave corners unattended. And as we discussed here earlier, we talked about perimeter threats and there might be some others. And a much more comprehensive approach would allow us to evaluate and to run a more balanced system, which by the way will never be perfect.

Mr. ROTH. I think any time that you add size, you get complexity, and so enhanced complexity of course always leads to challenges, but to your specific question, unfortunately we haven't done any specific work in that area so it's difficult for me to comment.

Ms. KELLY. Thank you for your response, I appreciate it. I yield back.

Mr. MICA. Mr. Cummings. Thank you.

Mr. CUMMINGS. Ms. Grover, are you familiar with the concerns the GAO raised about the Managed Inclusion program?

Ms. GROVER. Yes, sir.

Mr. CUMMINGS. Can you explain what steps TSA is taking to address those concerns?

Ms. GROVER. What TSA has told us is that they have an effectiveness study underway and they expect to have results toward the latter half of 2016. I believe specifically they are evaluating the role of the behavior detection officers and K–9, the K–9 teams as part of that.

Mr. CUMMINGS. So the DHS inspector general recommended that the Managed Inclusion program be halted until technology exists to connect Secure Flight data to airport checkpoints. And this would prevent passengers that are known security threats from trespassing—bypassing rather more rigorous security inspections according to the IG.

Now, Mr. Roth, has TSA halted the Managed Inclusion program?

Mr. ROTH. My understanding based on conversations with TSA is that they are reducing both Managed Inclusion and some of the other methods they use to put people into expedited screening. And as more people apply to PreCheck and get vetted they are going reduce that. But it is still something that they use, something that we are concerned about.

Mr. CUMMINGS. And tell me what your concerns are?

Mr. ROTH. Well, my concerns are that these are unknown passengers, they are unknown to TSA, which means they are unknown risk. And any time you have an unknown risk passenger going through expedited screening, which is inherently less secure, you have a security vulnerability.

Mr. CUMMINGS. And what have they done about your concerns?

Mr. ROTH. Well, we made a number of recommendations, again many of those are nonpublic recommendations, but they've largely nonconcurred with those recommendations, which we believe shows a lack of appreciation of the seriousness of the problem.

Mr. CUMMINGS. And did they give you excuses or what I mean——

Mr. ROTH. They simply disagree with the level of risk. They believe it is a level of risk that's acceptable. As the IG I believe that it is not. One of the reasons I invite a classified briefing on this is because every time I give a classified briefing, Members of Congress tend to agree that it is an unacceptable risk.

Mr. CUMMINGS. So you think they just discount your concerns? Do you get the impression that they don't see you as the expert and they see themselves as so being?

Mr. ROTH. Well, we're the independent auditor, so that means we are objective and we look, you know, while we are in——

Mr. CUMMINGS. That's not what I asked you.

Mr. ROTH. I apologize for that. Yes, we have a disagreement, a fundamental disagreement about what level of risk is acceptable.

Mr. CUMMINGS. So now, let's go to this issue of the perimeter, Mr. Roth. We've seen a disturbing report of a 15-year-old boy who traveled from San Jose International Airport to Hawaii in a wheel well of an aircraft. Mr. Roth, what steps can TSA take to improve perimeter security and ensure that incidents like this don't happen in the future. What can they do?

Mr. ROTH. My understanding of TSA's position is that, that is the responsibility of the airport itself and not of TSA. We have not looked at that specific issue, so I don't have any specifics with regard to their response.

Mr. CUMMINGS. Mr. Ron, do you have an opinion on that?

Mr. RON. Yes, I think that this is one of the problems that we have and this is why it falls between the chairs because why TSA does not consider it part of its responsibility. I think as a regulator it has to make sure that somebody else does it, and at the moment this is not really happening. The airports are not willing and in many cases are unable to provide what it takes to protect their security with an intrusion detection systems and the manpower that requires to respond to alarms.

Mr. CUMMINGS. And how is that done in other airports where you've been?

Mr. RON. Well, if I take for example Tel Aviv airport, Tel Aviv airport there is no division of responsibility. The responsibility structure is very, very clear and there's only one security organization that takes care of all aspects of security, whether it is passengers or the facility, and that makes it much easier to calculate the priorities.

Mr. CUMMINGS. So Mr. Roth, whose responsibility did they say it was, the perimeter?

Mr. ROTH. My understanding is that TSA takes the position that it's the airport's responsibility and not TSA's. Again, that's based on my understanding, but we haven't done any work in this area.

Mr. CUMMINGS. Ms. Grover, you want to say something?

Ms. GROVER. Yes, sir, if I may. TSA does take the position that it is the airport's responsibility to decide how their perimeter will be secured. What TSA does is they come in and they check—they do a paper check essentially to say given what the airport has decided to put in place for the perimeter, does that match up with the requirements? And then they also do an annual compliance inspection where they actually observe to make sure that those measures are in place. And we do have a study underway now to do an assessment of what is going on.

Mr. CUMMINGS. Wait a minute, back up.

Ms. GROVER. Yes, sir.

Mr. CUMMINGS. You said they—they—TSA says this is what we think it ought to be; is that right?

Ms. GROVER. Yes. Yes, sir, there are regulations, and then TSA issues security directives, for example, that lay out sort of at a high level what the requirements need to be to secure the perimeter. And then at each individual airport, the airport decides exactly how they are going to meet that requirement.

Mr. CUMMINGS. OK.

Ms. GROVER. Right. So it could be a fence or maybe the airport would say, well, we don't really need a fence because we have a body of water there. So then TSA comes in and they review that airport's security program. That's a paper review where TSA basically says, check, check, check, check, check. OK, yes, we think it's reasonable that you are securing your perimeter in all of these ways. And then once a year TSA also comes in and does a compliance inspection where they say walk—they walk the perimeter and they confirm is the fence there and does it have holes in it.

Mr. CUMMINGS. What happens the day after the inspection somebody cuts a hole in the fence? I mean, how does that work? And do we then have a gap?

Ms. GROVER. That is the airport's responsibility to monitor.

Mr. CUMMINGS. Yes. You know, one of the things that concerns me, and we saw this on the Transportation Committee, you have these folks who constantly claim that everything is tight and there are no problems and then they say when the rubber meets the road, everything is going to be fine. But then we find that there are gaps because everybody is assuming that the other person's doing it, and then it ends up that there is a problem.

And I am just wondering, you know, if you have—I mean, when we look at what's happening around the world and we look at organizations like ISIS and others, I mean, to create a hole in a fence and folks figure out well, maybe they are not looking at that fence as often as they should. They had an inspection yesterday and now I have got a whole year to wait. Are you satisfied with that procedure or you don't get into that.

Ms. GROVER. So there are definite vulnerabilities, and we have identified them before, and we have called out to TSA and let them know that we didn't think that they had sufficient vulnerability assessments in place to check on the airports. So that's part of the issue we are going to be looking at again right now, and we would be happy to report back to you on it.

Mr. CUMMINGS. Yes, I would love to have that, because that's of great concern. Thank you all very much, your testimony has been very informative.

Mr. MICA. Thank you. Mr. Cummings. If you could—if you could patch that fence, then you could put five pounds of plastic explosives on a drone, and drive it into an airplane as it's taking off or use shoulder fired missile, come into the market, do the same thing. It all gets back to intelligence, finding these people before they can commit the act.

Mrs. Lawrence you're recognized,

Mrs. LAWRENCE. Thank you, Mr. Chair. Talk about the issue of access through the IDs, on March 9, 2015, NBC News reported that 1,400 badges that granted access to secure areas had gone missing over a 2-year period. Are you familiar with this report, Mr. Roth?

Mr. ROTH. I am.

Mrs. LAWRENCE. What happens when an ID badge is lost or reported stolen?

Ms. GROVER. So as soon as the badge has been reported lost or missing, then the airport should deactivate it immediately. It's my understanding that there's a threshold of 5 percent. So once 5 percent of the badges for any particular area have been reported as

missing, then the airport is responsible for reissuing all of the badges to all the employees who have access in that area.

Mrs. LAWRENCE. Do you know how the airports keep track of this? Are you engaged in that tracking process?

Ms. GROVER. So we have not done a specific review of how well the tracking process is working, but I can tell you generally that the way it works is that the airports are required to do a 100 percent audit of the badges once a year. That's a paper exercise, so it involves the airport taking a list of all of the badges that have been issued and checking it up against the contractor lists to say, do our lists still match? And then twice a year they do an additional 10 percent random sample, that's also a paper exercise. And TSA's responsibility is to come behind and make sure that the airport has done their job in doing those checks.

Mrs. LAWRENCE. So that's my followup. When the TSA is supposed to come behind, so there is an audit process that is given to any airport. Is there an inspection process? How do you know that—how do you verify that the airports are in compliance, because the concern that we have about these missing ID badges is we provide all the security under TSA that we have the expectations, how do—how does TSA verify that there's an inspection needed because the audit has failed? And what is the procedure?

Mr. ROTH. It's a couplefold. It's my understanding is that TSA will go through and they will in fact audit these things and have an entire office of inspection——

Mrs. LAWRENCE. How frequently?

Mr. ROTH. I don't have the answer to that. One of the other things that we do, for example, what we are doing now is we are conducting an independent audit of TSA's processes and controls for doing this. We were as concerned as I suspect you were with regard to the media reports. And so we are taking a look at that very issue.

Mrs. LAWRENCE. I just want to say that I'm glad to hear that you are conducting the audit of that process. It is disturbing to me that the access to secure areas, this number is too high. And in doing that audit I really want to State for the record that I feel it's too high. You're going to have to convince me otherwise.

And things like the frequency, when is there accountability issued for the airports and for employees for these loss of badges. And the question of the answer after a certain period that everyone gets their badges reissued, how frequently is that happening? And what triggers that number?

So those are the concerns I have. As we are—it should be a comprehensive approach. I would hope that the media would not drive our response to these issues, that's troubling to me. It should have been something that has been triggered by our own internal audits, if we are doing that, instead of saying, oh, it's in the media now, we need to respond. So thank you.

Mr. MICA. I thank the gentlelady, and I guess there are no further members. I'll conclude the hearing, but it's not acceptable for TSA to respond to the chief investigative and oversight of Congress Committee with pages and pages of redacted information. Do you have trouble, Mr. Roth, getting information from them or——

Mr. ROTH. We do not.

Mr. MICA. You do not, but we do. And your report I think it is about as comprehensive as I have seen. It covers a whole host of areas. I think you did an excellent job. The problem is it just highlights that after years and years, we have created a very expensive, dysfunctional, transportation security system, and there are many potentials for risks that are not addressed.

The more I—on having helped create TSA in the beginning and create the system, the more I look at this the more I am convinced that you go back to intelligence, intelligence, intelligence. Get TSA out of the screening business. As you heard Mr. Ron say, we're the only country in the world that the—where the agency is the regulator, the auditor, the systems manager, and it doesn't do any of them well.

But if we could concentrate on connecting the dots so that we have the information in the data base that we can clear people we know who's traveling and poses a risk. If we can track people. Almost everyone most recently that—Boston bombers, other people, we failed to connect the dots. The dots were there. But we have concentrated a huge number of people in managing an unmanageable system that others can do to conduct a screening process through, then concentrate on getting the intelligence, the security information setting the protocols and altering them to meet the threat. Mr. Ron, isn't that what we should do?

Mr. RON. Yes.

Mr. MICA. I didn't want to take words out of your mouth.

Mr. RON. Relatively speaking, yes.

Mr. MICA. Yes. And the Israelis have done a great job. They have a different system, been there many times. After 9/11 they helped us in many areas and have continued to lend their expertise. And I can tell you, and in this hearing, if it wasn't for Israeli intelligence and British intelligence we would have been taken down several times, because they don't have to deal with some of the laws and protections and barriers that we have, because we have a different society and different laws.

But this is a very serious situation. This is an indictment of TSA's values and we need to change this. I've never said to do away with TSA, we need to change their role so that they are in charge of again security, intelligence, connecting the dots, and then auditing the system and getting out of this craziness that is using all of our manpower and money for a system that shakes down little old ladies, veterans, and people who pose no risk. And Mr. Roth agrees with that Statement, don't you, Mr. Roth?

Mr. ROTH. Yes, sir.

Mr. MICA. OK. Ms. Grover is a little bit hesitant but she might agree.

Ms. GROVER. We agree that there are vulnerabilities in the system that definitely need to be addressed.

Mr. MICA. Need to be addressed.

Ms. GROVER. Yes, sir.

Mr. MICA. So with those Statements what I am going to do is ask unanimous consent that the record be left open for a period of 10 business days. You may get additional questions, and I think there will be some coming to TSA, maybe wrapped in a subpoena for Mr.

Carraway, but in any event the record will be left open. Without objection, so ordered.

Mr. MICA. There being no further business before this full Committee hearing of Government Oversight and Reform Committee and the Subcommittee on Transportation and Public Assets, this hearing is adjourned. Thank you.

[Whereupon, at 12:19 p.m., the subcommittee was adjourned.]

# APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Timeline of OGR Interaction with TSA/DHS

- **Wednesday, April 08, 2015 10:35 AM**: OGR asks TSA if AA Carraway is available for an April 22 Subcommittee Hrg on airport security.

- TSA replies noting 3 week notice is their policy.

- OGR agrees to allow the Deputy to testify instead of Carraway for the Subcommittee hearing.

- **Fri 4/17/2015 9:27 AM**: OGR emails following up on a voicemail notifying TSA the hearing has been moved to the Full Committee and tells TSA of the new date, May 13.

- April 17, OGR emails formal invitation letter to Carraway.

- **Thursday, April 30, 2015 9:53 AM**: TSA emails OGR with concerns over the panel, specifically saying they do not send witnesses to sit on a panel with any non-government witnesses.

- May 6, OGR calls TSA to discuss panel concerns. TSA states on the call, sitting with non-government witness "denigrates the office."

- **Mon 5/11/2015 10:49 AM**: OGR emails TSA again stating the Committee's position with the panel: it will be one.

- **Mon 5/11/2015 3:37 PM**: DHS emails OGR stating it will not send AA Carraway to the hearing due to the paneling concern.

- May 12, OGR calls DHS to reiterate the expectations of Carraway testifying.

- **Tue 5/12/2015 4:12 PM**: DHS emails, "The Department is not going to provide the Acting Administrator for tomorrow's hearing but will allow the Deputy Administrator, Mark Hatfield, to testify. This should not be considered precedent setting; our hearing policy will continue to apply. Hopefully, however, this will allow the Committee to have a productive conversation about aviation security tomorrow."

- **Tuesday, May 12, 2015 5:02 PM**: OGR responds, "The invitation was to Acting Administrator Carraway and per previous conversations, the chairman still expects him to testify."

- **Tue 5/12/2015 5:31 PM**: DHS emails, "Acting Administrator Carraway is out of town all day tomorrow and is not available. Deputy Administrator Hatfield will be in the hearing room at 10 AM, prepared to give testimony. As you no doubt know, Mr. Hatfield was FSD at JFK, Miami, and Newark, among other jobs at TSA, and so will be very well-prepared to speak to the Committee's interests."

**Statement of Congressman Gerald E. Connolly (VA-11)**
**Committee on Oversight and Government Reform**
***Transportation Security: Are Our Airports Safe?***
**May 13, 2015**

Chairman Chaffetz and Ranking Member Cummings, thank you for holding today's hearing to examine transportation security at our Nation's airports. The performance of the U.S. Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has been controversial since the inception of the agency. Reviews and audits conducted by the U.S. Government Accountability Office (GAO) and the DHS Office of Inspector General (DHS OIG) demonstrate that TSA faces serious challenges in effectively safeguarding domestic air travel and that much work remains to be done in the coming years.

It is absolutely vital that we secure our Nation's ports of entry against infiltration by our adversaries. Every day, TSA faces a tremendous challenge in facilitating the safe and free movement of more than 1.8 million passengers and nearly 3 million carry-on bags through America's air transportation system. As the DHS Inspector General will testify this morning, "...we face a classic asymmetric threat in attempting to secure our transportation security: TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, yet a terrorist only needs to get it right once."

TSA's 50,000 Transportation Security Officers (TSOs) tasked with screening passengers at 450 airports clearly have the incredibly daunting task of having to remain vigilant and alert through long hours of conducting what most observers would concede are tedious and often mundane tasks. I remain concerned about the quality of customer service provided by TSOs across the country, and look forward to examining how much progress TSA has made in improving its customer service training and the agency's monitoring of this performance metric.

Of course, I also recognize that passengers have a role to play in facilitating excellent customer service, and it is reasonable that if the traveling public is to demand that TSOs simultaneously stand vigilant against national security threats while ensuring pleasant interactions with non-threatening travelers, the least passengers can do is to treat TSA personnel with respect and dignity – which similar to those TSOs that fall short of acceptable customer service, regrettably, does not always take place. The bottom line is that safeguarding our national and economic security requires that we all work together to carry out this incredibly important mission.

Unfortunately, both the GAO and the DHS OIG will testify today that TSA continues to experience significant shortfalls across its programs and general management practices. For example, the prepared statement of the DHS IG for this hearing notes, "Despite spending billions on aviation security technology, our testing of certain systems has revealed no resulting improvement," while the GAO notes in its testimony that it has recommended Congress limit future funding of TSA's Behavioral Detection Officer program because the agency has failed to

scientifically validate that behavioral indicators can be used to identify passengers who pose a threat to transportation security.

These types of findings are disappointing and frankly, very alarming. I, for one, want to know why to date, TSA has not fully concurred with many of the DHS OIG and GAO findings and recommendations. America's ports of entry remain a prime target and viable pathway through which terrorists can infiltrate and attack our homeland. TSA must do everything in its power to continually improve its effectiveness.

I look forward to hearing from our witnesses about the specific steps this Committee can take to ensure that TSA better safeguards our economy, our ports of entry, and most importantly, the American people.

**Statement of**

**Transportation Security Administration**

**U.S. Department of Homeland Security**

**Before the**

**Committee on Oversight and Government Reform**

**U.S. House of Representatives**

**May 13, 2015**

Good morning Chairman Chaffetz, Ranking Member Cummings, and distinguished members of the Committee. Thank you for the opportunity to appear before you today to discuss Transportation Security Administration's (TSA) efforts in securing our nation's transportation systems.

TSA is a high-performing counterterrorism organization, applying a multi-layered, intelligence-driven, risk-based approach to securing aviation, mass transit, rail, highway, and pipeline. TSA could not accomplish this essential mission without a workforce trained, equipped and committed to the safety and security of this Nation. Every TSA employee remains steadfast in the face of a threat that has not diminished more than a decade following the terrorist attacks on September 11, 2001. In fact, over the years, the adversary has become more inventive and persistent, while at the same time growing and spreading to other countries and regions. We continue to face a real and persistent threat from adversaries adept in the design, construction and concealment of explosives. As such, TSA is evolving our approach to transportation security and to mitigate risks we all face when traveling from, within and to the United States.

In pursuit of TSA's mission, in FY 2014, Transportation Security Officers screened approximately 650 million passengers and more than 2 billion carry-on and checked bags,

preventing approximately 105,000 dangerous prohibited items, including 2,300 firearms, from being carried onto planes. TSA also screened a daily average of 6 million air passengers against the U.S. Government's Terrorist Screening Database.

Additionally, Federal Air Marshals flew thousands of flights, domestically and internationally, providing in-flight security for high risk routes; Visible Intermodal Prevention and Response teams conducted almost 17,000 operations; Transportation Security Inspectors completed over 1,054 airport inspections, 17,894 aircraft operator inspections, and 2,959 foreign air carrier inspections to ensure compliance with rules and regulations; and TSA's vetting systems recurrently vetted 14.8 million transportation worker records each day against the Terrorist Screening Database.

**Risk-Based Security (RBS)**

TSA uses multi-layered, intelligence-driven, and risk-based initiatives to enhance security. These risk-based initiatives direct resources focused on high-risk and unknown travelers and commerce, while at the same time facilitating the movement of legitimate travelers and trade. RBS methods have proven more efficient in moving people through the checkpoint than standard screening lanes, requiring fewer screeners and fewer lanes than traditional screening operations to provide the most effective security in the most efficient manner. As a result, TSA continues to gain efficiencies through RBS initiatives, with savings of approximately $350 million over the past two years at airports.

In December 2013, TSA launched our TSA Pre✓® application program, which is the cornerstone of our expedited screening efforts. TSA Pre✓® is one of the Department of Homeland Security's expedited screening enrollment programs, and was one of the first

initiatives in TSA's shift toward a risk-based and intelligence-driven approach to security. Through this program, U.S. citizens and lawful permanent residents can apply directly to participate in TSA Pre✓® and undergo a background check in order to become eligible for a period of 5 years. Passengers may qualify for the program either directly through the TSA's Pre✓® application program, or through the U.S Customs and Border Protection's (CBP) Trusted Traveler Programs (Global Entry, SENTRI, and NEXUS).

TSA has worked closely with U.S. and foreign airlines to expand the number of airlines participating in TSA Pre✓®, and has extended eligibility for TSA Pre✓® to U.S. Armed Forces personnel, Department of Defense personnel, and U.S. Coast Guard civilian employees. More than 60,000 DOD employees benefit from TSA Pre✓® each week, and that number continues to steadily increase. TSA continues to expand the prescreening process by increasing the number of known, lower-risk travelers eligible for expedited screening. Today, over 1 million applicants are enrolled in the program.

This year, TSA will continue to focus on increasing participation in TSA Pre✓® with the goal of providing expedited screening to a majority of the traveling public. We plan to accomplish this by identifying and enrolling more low-risk populations, expanding participation to additional U.S. and foreign airlines, exploring potential opportunities to leverage private sector capabilities and expertise in the TSA Pre✓® application process, and offering additional opportunities for enrollment in TSA Pre✓®.

**Access Control and Employee Screening**

Each day, TSA facilitates and secures the travel of nearly 2 million air passengers at 441 airports nationwide. Controlling access to sterile (post-security screening checkpoint) airport

areas is a critical part of airport operations. While the sterile area hosts passengers and air crews waiting for flights, it is also the workplace for vendors, mechanics, ground crew, and others employed by the airlines and the airports. Access control is a shared responsibility among many partners, and every airport and airline has a security plan of which access control is an important and necessary element. Airport authorities and the airlines are responsible for developing and executing security plans; TSA is responsible for approving security plans and inspecting for compliance.

TSA's inspections include credentialing, perimeter security and testing of access control systems and processes at airports. Every commercial airport receives an annual security inspection to include an assessment of perimeter and access controls. TSA analyzes the results of these inspections and assessments to develop mitigation strategies to enhance airport security.

Transportation Security Officers and Inspectors are also deployed on a random and unpredictable basis to screen airport and airline workers as they enter for work within the secure and sterile areas. The screening protocols vary by time, location, and method to enhance unpredictability. This includes ID verifications, and searches of individuals and/or their property, using various technologies and methods in order to detect and deter the introduction of prohibited items. Additionally, airport operators are required to conduct random inspections of employees entering sterile areas, to include ID verification and checks for prohibited items. If employees fail to follow proper procedures in accessing secure areas, they may be restricted from future access, disciplined by their employer, or subject to criminal charges and civil penalties.

TSA has wide ranging authority to pursue inspections of airport security plans. Each airport operator is required to allow TSA, at any time or place, to make any inspections or tests,

to determine compliance of an airport operator, aircraft operator, foreign air carrier, indirect air carrier, or other airport tenants with TSA's regulations, security programs, security directives, and other policies. Inspections and audits are conducted by our Compliance Division and, in situations of possible non-compliance, investigations are undertaken by Transportation Security Inspectors. Enforcement Investigation Reports that yield evidence of non-compliance are jointly overseen by the airport's Federal Security Director and by the Office of Security Operation's Compliance Division.

**Vetting and Badging Process**

In addition to our regulatory role, TSA also conducts security background checks for airport and airline employees through the Secure Identification Display Area (SIDA) badging process. Airport workers are vetted before they are granted unescorted access to the secure area of the airport. TSA performs a Security Threat Assessment (STA) on those who require access to the secure/sterile area of the airport or unescorted access to cargo. When individuals apply for employment with the airport or airline, they submit information which is passed through one of several vendors to TSA for adjudication. This includes a check against the Terrorist Screening Database (TSDB). In partnership with the FBI and CBP, the individual also undergoes a Criminal History Background Check and immigration status check. Once TSA has completed the check, the information is provided to the individual's prospective employer with access either granted or denied based on the results of the STA. TSA also continuously checks all SIDA holders against the TSDB for any changes in status.

With TSA's Risk Based Security model, similar to what we do with travelers in TSA Pre ✓®or Known Crew Member, airport workers are vetted before they are granted unescorted

access to the secure area of the airport. With the STA, TSA focuses on a variety of threats to aviation security, which is particularly important given the sensitive areas where many of these individuals work. We also remain cognizant of the importance of balancing security with commerce and, and have designed a system of inspections, and random checks as a risk-based approach to access control.

**Aviation Security Advisory Committee (ASAC) Report**

While the measures TSA has in place for background checks, security programs, and compliance inspections provide a good baseline for access control security, the December incident of an alleged gun smuggling ring at ATL illustrated a need to consider options to close the potential vulnerability of a terrorist utilizing insider threat methods. The ASAC was the ideal consultation approach to access control vulnerabilities as their membership of industry, law enforcement, and other key stakeholders brought a broad range of perspectives to the problem of insider threat and access control. I am pleased to note that the recommendations in their 90 day review are comprehensive, thoughtful, and will help TSA achieve meaningful reforms in partnership with our aviation stakeholders. Additionally, these recommendations use a risk-based approach, allowing resources to be used in the most efficient way for the most effective security. The ASAC identified five areas where TSA and industry can take action to address potential vulnerabilities. These areas are:

- Security Screening and Inspection
- Vetting of Employees and Security Threat Assessments
- Internal Controls and Auditing of Airport-Issued Credentials
- Risk-Based Security for Higher Risk Populations and Intelligence

- Security Awareness and Vigilance

TSA appreciates the ASAC's timely and thoughtful review, and looks forward to working with them and our industry partners to explore implementation of these recommendations.

As a result of ASAC's review, on April 20, 2015 Secretary of Homeland Security Jeh Johnson announced a number of additional steps TSA will take to address the potential insider threat vulnerability at U.S. airports. First, until TSA establishes a system for real time recurrent criminal history background checks for all aviation workers, we will require airports and airlines to conduct fingerprint-based Criminal History Records Checks every two years for all employee SIDA badge holders. We will reinforce existing requirements that all airport and airline employees traveling as passengers are screened by TSA prior to travel. We will direct and work with airports to reduce the number of access points to secured areas to an operational minimum. Additionally, TSA will require airports to increase aviation employee screening, to include additional randomization screening throughout the workday. Finally, we will work with our stakeholder partners to emphasize and leverage the Department of Homeland Security's "If You See Something, Say Something™" initiative to improve situational awareness and encourage detection and reporting of threat activity.

These enhancements to access control nationwide will greatly improve our effectiveness by reducing vulnerabilities and maintaining our risk-based approach to aviation security. Over the coming months, TSA will examine additional recommendations to implement in the future to continue strengthening our nation's airports. I appreciate the ASAC's timely and thoughtful review, and look forward to working with them and our industry partners.

Of note, the ASAC held the consensus opinion that while physical screening of employees is one means of deterring terrorist activity, 100 percent physical employee screening is not the only, or necessarily the best, solution. Requiring 100 percent physical employee screening would divert limited resources from other critical security functions. Such physical screening, moreover, would require infrastructure improvements, workforce expansion and airport reconfiguration. This would constitute an ineffective use of resources with limited security value. An ASAC working group concluded that "the provision of so-called '100 percent measures' as a layer of airport security does not appreciably increase the overall level of system-wide protection, nor does it lower over-all risk." It concluded that a random and unpredictable screening strategy would be the most cost-effective solution.

**Conclusion**

TSA plays an important role in partnership with airports and airlines in securing access to our Nation's airports, and is committed to fielding responsive, risk-based solutions that can enhance our current security posture. I want to thank the committee for your interest in TSA's efforts to improve aviation and airport security nationwide. Thank you for the opportunity to testify today, I look forward to your questions.